

**DESIGN AND IMPLEMENTATION OF A NETWORK SECURITY MODEL
FOR THE EXIM BANK NETWORK**

Submitted By

Golam Rabby Chowdhury

ID: 163-15-8326

A Project Report Submitted in partial fulfillment of the requirements for the
Degree of Bachelor of Science in Computer Science & Engineering

Supervised By

Refath Ara Hossain

Lecturer

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH


September, 2019

DECLARATION

I, hereby declare that the work presented in the internship report is the outcome of the investigation performed by under the supervision of **Refath Ara Hossain** Lecturer, Department of Computer Science and Engineering Daffodil International University

I also declare that no part of this project has been or is being submitted elsewhere for the award of any degree or diploma.

Supervised by:

 15.09.2019


Refath Ara Hossain

Lecturer

Department of CSE

Daffodil International University

Submitted by:


Golam Rabby Chowdhury

ID: 163-15-8326

Department of CSE

Daffodil International University

ABSTRACT

In this internship, I have designed and implemented a secured computer network for a company. I have used VLSM, VLAN, cisco routers and switches and firewalls to implement and configure the network. I have studied the types of threats a computer network may face and their implications on the performance of a computer network. I configured the firewalls with access control list (ACL) such that unauthorized access to the network can be minimized. I have used cisco packet tracer to simulate the design and the configurations of the network.

ACKNOWLEDGEMENT

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

I really grateful and wish our profound our indebtedness to **Supervisor Refath Ara Hossain, Lecturer**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of Networking” to carry out this internship. Her 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.

I would like to express our heartiest gratitude to **Dr. Syed Akhter Hossain, Professor and Head, Department of CSE**, 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.

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

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

TABLE OF CONTENTS

CONTENTS	PAGE
Approval	i
Declaration	ii
Abstract	iii
Acknowledgement	iv
Chapter 1: Introduction	1-3
1.1 Introduction	1
1.2 Motivation	2
1.3 Internship Objectives	2
1.4 Report Layout Chapter	3
Chapter 2: Organization	4-8
2.1 Introduction	4
2.2 Product and Market Situation	5
2.3 Target Group	6
2.4 SWOT Analysis	7
2.5 Organizational Structure	8
Chapter 3: Tasks, Projects and Activities	9-10
3.1 Daily Task and Activities	9
3.2 Events and Activities	9
3.3 Project Task and Activities	10
3.4 Challenges	10
Chapter 4: Competencies and Smart Plan	11-14
4.1 Competencies Earned	12
4.2 Smart Plan	13
4.3 Reflections	14

Chapter 5: Conclusion and Future Career	15-16
5.1 Discussion and Conclusion	15
5.2 Scope for Further Career	16
Reference	17
Appendix	18

List of Figure

Figure	Page
2.1 Flow Chart of connectivity of server	4
2.2 VLAN Configure	5
2.3 Flow Chart of proposed VLAN	6
2.4 Flow Chart of Proposed Network Diagram	8
3.1 OSF	10
4.1 Firewall	11
4.2 Security Zones	13
4.4 Firewall Design	14

CHAPTER 01

Introduction

1.1 Introduction

Internet and networks in the local area security is now associated with the computer network. Information and networking threats have increased dramatically. Many of these threats have become clever attacks that cause harm or theft. The Internet is exponentially growing. As the government becomes more involved in business-critical apps on the Internet, there are more instant advantages. These network-based apps and services, however, can present safety hazards for people to company and government information resources.

Many companies and governments risk losing that asset without adequate protection and network security. Network security is the very method through which digital data assets are protected, the most important security objectives are confidentiality protection and accessibility. With this in mind, it is essential that all networks are protected against threats and vulnerabilities in order to maximize the potential of a company.

1.2 Network security

A specific area of computer networking involving the securing of the infrastructure of the computer network. Network security is an organization's approach that guarantees network security safety of its resources including all network traffic. Typically, network security is addressed through a network administrator or system administrator implementing security policy, network software and hardware required to protect the network and resource policies accessed through the network from unauthorized access and to Ensure appropriate network access and network resources are available to staff. Our world has been converted by digitization. Everything has changed how we live, work, play, and learn. Any organization that wishes to provide the services required by clients and staff must safeguard its network. Network security also helps safeguard against attack proprietary data. In the end, it safeguards your reputation.

1.3 Advantages of Network Security

Business computer networks experience fresh threats every day, such as intrusions of spyware, malware, and hacker. Protecting your business network is more IMPORTANT than ever before the need for Network Security cannot be denied. With a system of network security, all the files, Data and private information are kept secure and protected from unauthorized access by individuals on the network and outside the network. That's why it's commonly used in offices, banks, and many others Network Security regulations and policies assist the network administrator track any type of computer network misuse, alteration or unauthorized access. This prevents a number of cyber-attacks and other damaging operations.

Protect data: Network security checks unauthorized access as discussed. A network includes many private information, such as private customer information. Those delicate information may be hampered by anyone breaking into the network. In order to safeguard them, network security should be in place.

Prevents cyber-attack: Most of the network assault comes from the internet. Hackers are specialists in this and then virus assaults take place. They can play with a lot of data in the network if careless. Network security can stop pcs from being harmed by these assaults.

Levels of access: Security software provides distinct users with distinct rates of access. The user's authentication is accompanied by the authorization method in which it is verified whether the user is allowed to access certain resources. You may have seen some password protected for safety in shared documents. The software understands obviously which funds are available to whom.

Centrally controlled: Unlike the desktop safety software, a key customer named the network administrator controls the network security software while the former is prone to worms and virus attacks, the latter can prevent hackers from harming anything before they do. This is because in a computer with no internet, the software is mounted.

Lower Costs: It is more cost-effective to use a managed security service than to pay IT advisors on an hourly basis or keep a full-time employees. Lower spending means better results and more capacity to pass on these savings to your clients.

Reduced Stress: You will never lose sleep with Network Security over stressing the safety of your company. We're going to handle everything so you don't have to. Safe Now you have more time to concentrate on making your business even more successful because you know it's for safety purposes. In this tip, we will investigate why these systems are simple targets, how many of today's malicious network assaults are being carried out against routers, switches and firewalls ; and what a company can do to protect their network against them.

Chapter 2

Organization

2.1 Introduction

A server is a computer program or device in computer networking that gives a service to another computer program and its user, also known as the client. The physical computer running on a server program is also often referred to as a server in a data center. This computer can be a dedicated server or for other uses as well.

Servers include:

- Mail servers
- Test servers

This client-server networking model is used by numerous applications on the Internet, including websites and email services. Continue pressing next to the server connectivity chart shown in fig 2.1

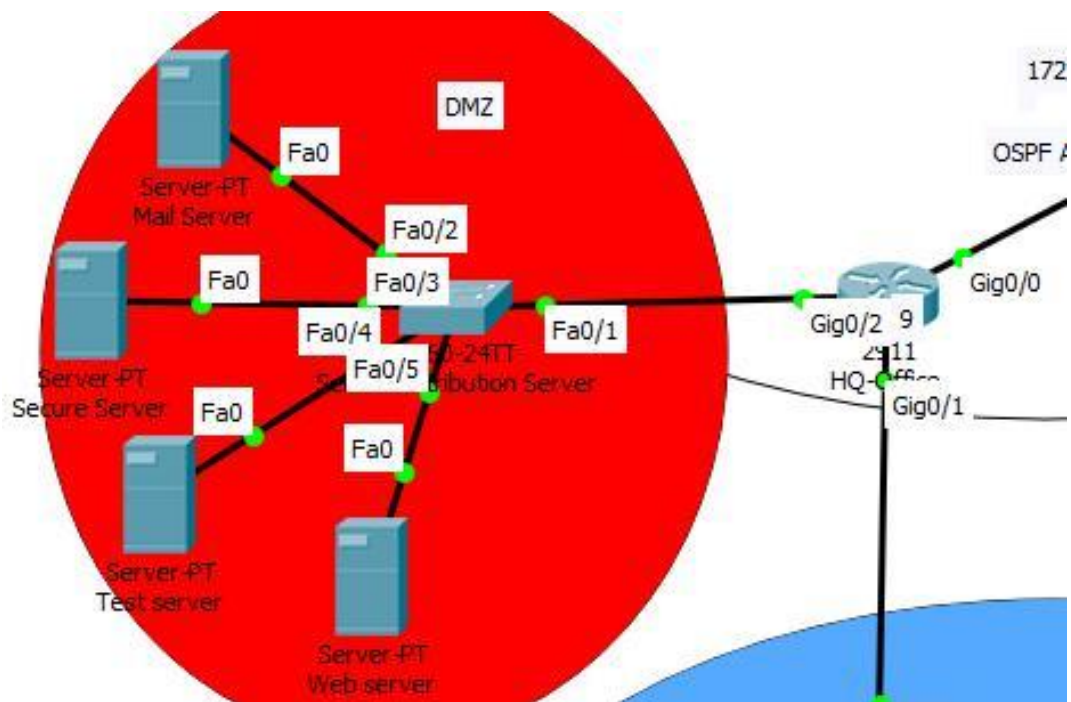


Figure: 2.1 Flow Chart of connectivity of server

2.2. VLAN Trucking

Without mentioning trunks, you cannot portray VLANs. It's a known fact that with VLANs you can regulate and segment network transmissions. VLAN trucking allows traffic to be moved to various areas of the network configured as a VLAN. Most Cisco switches support the IEEE 802.1Q used on Fast Ethernet and Gigabit Ethernet to coordinate connections.

2.3 Vlan Trunk port configuration

Trunks are frequently used between switches and other devices on the network like a router, another switch, or a server. A network engineer must be acquainted with the configuration and proper functioning of a trunk. VLAN Configure Figure 2.2 Continue

```
interface FastEthernet0/1
  switchport mode trunk
  !
interface FastEthernet0/2
  switchport access vlan 2
  switchport mode access
  !
interface FastEthernet0/3
  switchport access vlan 3
  switchport mode access
  !
interface FastEthernet0/4
  switchport access vlan 4
  switchport mode access
  !
interface FastEthernet0/5
  switchport mode trunk
  !
```

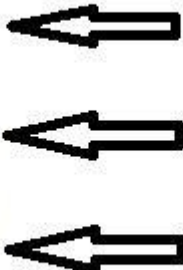


Figure: 2:2 VLAN Configure

2.3 Flow Chart of Proposed VLAN

Continue pressing shown in fig 2.3

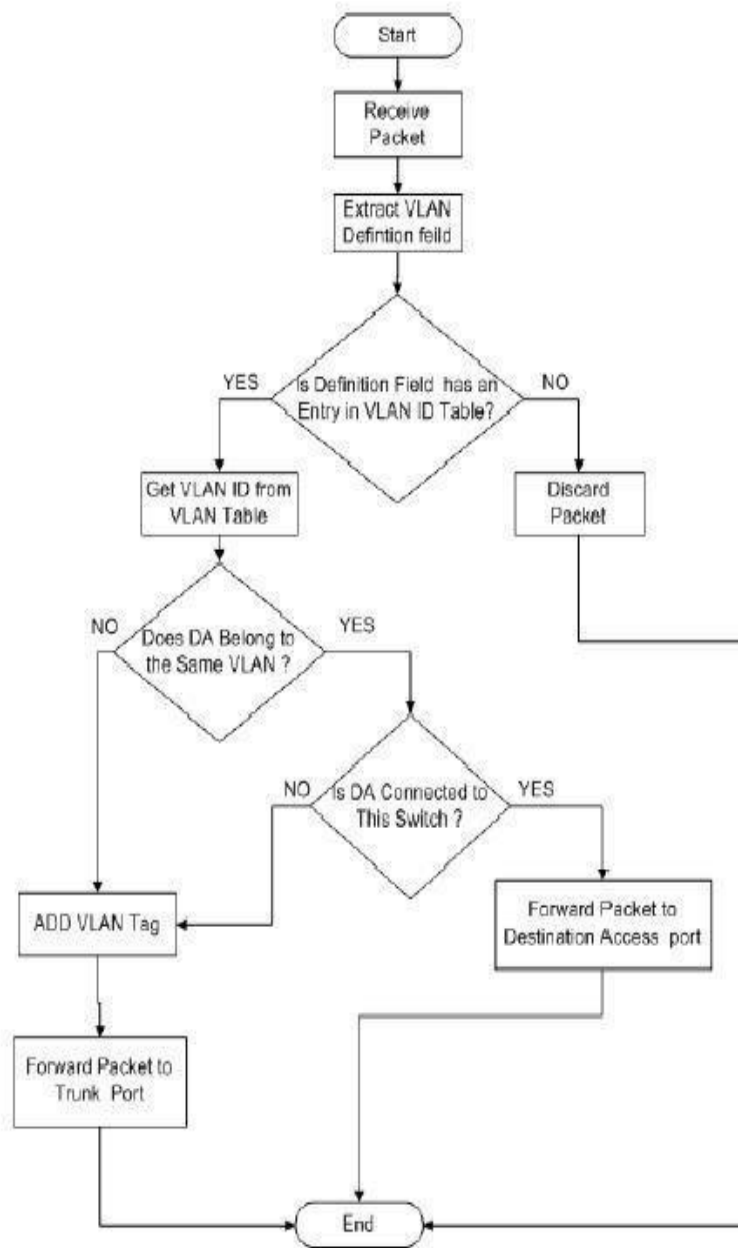


Figure: 2.3 Flow Chart of proposed VLAN

2.5 Variable Length Subnet Mask (VLSM):

VLSM, sub networks use requirement-based block size so various subletting is needed. Suppose there is an administrator responsible for managing four departments. These are department of sales and buy with 120 pcs, department of growth with 50 pcs, department of accounts with 26 pcs and department of leadership with 5 pcs.

1. Disabling all remote access non-IP-based to use Encryption of SSH or IP Security (IPsec)

all remote connections to the router instead of TELNET, this can provide complete VTYs protection. Remote administration is inherently dangerous because anyone with a network sniffer on the right LAN segment can acquire the router passwords and would then be able to take control of the router.

AAA will give more control and better audit. AAA is the acronym for authentication, author
2 Applied routing access control lists, malicious traffic packets filtering and tariff restrictions, this filtering can generally be performed on the basis of two networks the source and destination IP addresses to the traffic type.

3.The routing of access control lists can decrease all traffic to IP addresses of the internal networks that are not part of the internal networks, Reject all external network traffic with an inner network source address and Reject all traffic with a reserved, uncountable or unlawful address source or destination address.

4. Additionally configure Authentication Proxy to set up a router and firewall authentication account, local area database and authentication using AAA. This is the fresh access control facility for Cisco to control access, privileges and log customer activity on a router. Authentication is the user identification process before enabling access to a component of the network. Authorization is the technique used to define what a user is entitled to do after authenticating the router.

5. The use of Cisco IOS firewall IDS is an IDS intended to improve boundary routers in real time. Safety by detecting, reporting and stopping unauthorized activity. For many, but not all, Cisco routers, this facility is accessible in IOS versions. A distinctive advantage of applying an IDS on a router, particularly a boundary router, is that it flows through all network traffic and it is possible to examine it.

6. To mitigate CAM table overflow assaults, apply network security port on the switch. Once port security can be implemented in three forms: static, safe MAC addresses, dynamic and

safe MAC addresses. When a port security breach happens, the sort of action taken falls into the following three classifications: Protect, Restrict, Shutdown.

2.6 Proposed Network Diagram (Our Network Design)

Proposed Network Diagram In fig 2.4 Shows Flow Chart

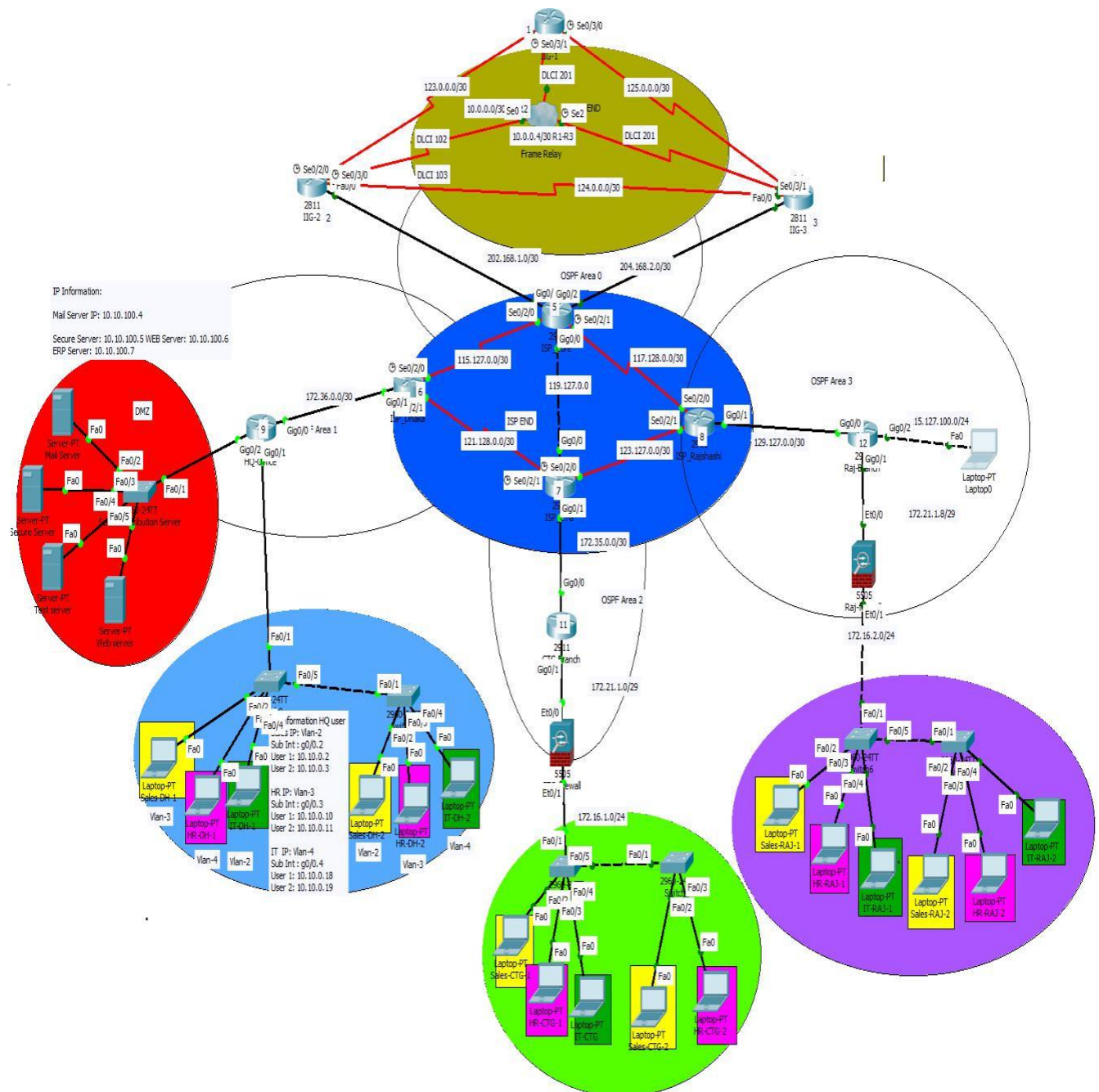


Figure: 2.4 Flow Chart of Proposed Network Diagram

Chapter 3

Tasks, Projects and Activities

3.1 Daily Task and Activities

You can find your IP location with our IP Lookup instrument. Due to many distinct variables, no IP Lookup instrument is 100% precise. People believe that if they search for an IP address, they will discover the user's physical address allocated to the IP. That's just not true. We are currently unaware of any IP address database that will provide you with the precise physical address of the IP address you are looking for. At best, you're going to get the precise town the IP user is in. For an accurate physical address, you must contact the ISP (Internet Service Provider) of the IP address in question.

IPsec protocols

It is used to safeguard an end-to-end discussion between two hosts. This protection ensures authentication only. IPsec handles only the payload of the IP datagram, inserting a header between the IP header and the upper IP concentrations. header is changed to indicate that the next header to be treated is the AH protocol (next header field) Then the entire resulting IP packet, with the exception of some mutable IP header field, is authenticated by the hashing process and sent to the destination In tunnel mode, an IP datagram is fully encapsulated in a new IP datagram using IPsec. The packet is sealed with an Integrity Check Value to authenticate the sender and prevent transit it modification encapsulating the complete IP header as well as the IP header. The payload enables source and destination addresses to differ from those of the packet (this enables tunnel formation)

3.4 Secure Shell (SSH):

The SSH (also known as Secure Shell) protocol is a technique for safe remote connection from one computer to another. It offers several alternative possibilities for strong authentication, and with strong encryption it protects communication security and integrity. It is a safe solution to unprotected login protocols (such as telnet, rlogin) and unsafe techniques of file transfer (such as FTP).

3.6 OSPF:

Open Shortest Path First (OSPF) is a connection-state routing protocol that uses its own Shortest Path First to discover the best route between source and destination router. OSPF is created as an Interior Gateway Protocol (IGP) by the Internet Engineering Task Force (IETF), i.e. a protocol to move the packet within a big autonomous system or routing domain. It is a network layer protocol that operates on the 89 protocol and utilizes the 110 AD value. OSPF utilizes the assigned router (DR)/Backup Designated Router (BDR) multicast address 224.0.0.5 for standard communication and 224.0.0.6 for updating.

It enables the network to send and obtain IP packets via the shortest path between source and destination depending on the price of the connection bandwidth. OSPF In fig 3.1 Shows Flow Chart

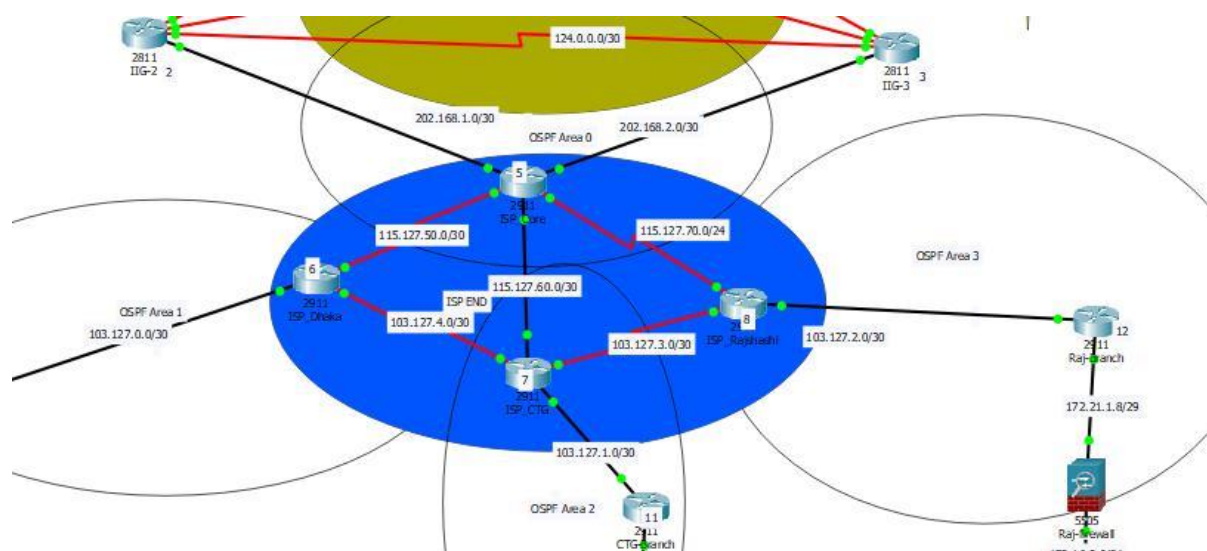


Figure: 3.1 OSPF

Chapter 4

Competencies and Smart Plan

4.1 Competencies Earned

The firewall is the obstacle between a trusted and untrusted network that is commonly used between your LAN and WAN. AWS Firewall Manager is a security management service that makes it simpler for your accounts and apps to centrally configure and handle AWS WAF rules. Firewall Is shown in fig 4.1

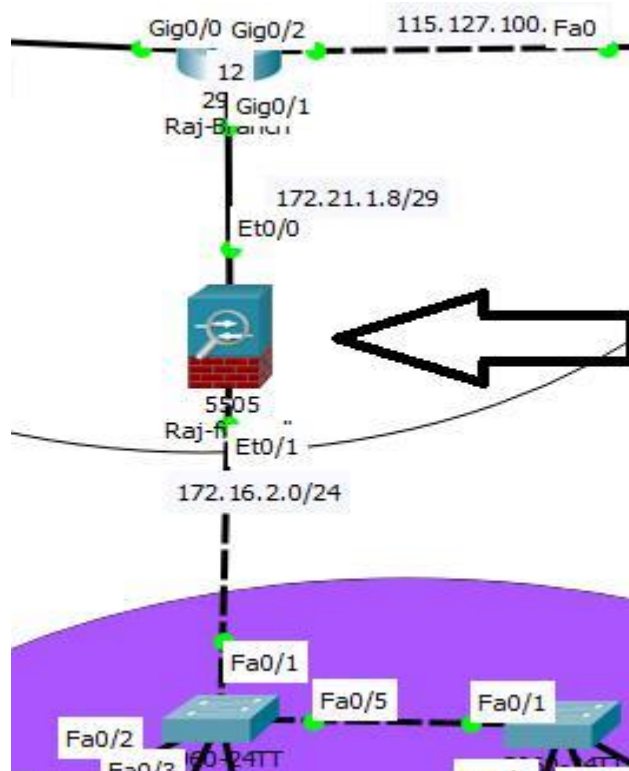


Figure: 4.1 Firewall

Above we have a host computer and a switch on our LAN. There is a router on the right that is attached to the ISP that provides Internet connectivity to safeguard our LAN, the firewall sits in between. The router is optional, depending on your WAN connectivity. For example, Firewall Manager also makes it easy to comply with a common set of security rules from day one with new applications and resources you now have a single service for building firewall regulations, creating security policies, and enforcing them in a coherent way. If you do any (advanced) routing like BGP, you will likely also need the router. Some fundamental routing alternatives are

supported by most firewalls: static routes, default paths and sometimes routing protocols such as RIP, OSPF or EIGRP.

4.1.2 Tasteful Filtering

Like routers, access lists can be used by firewalls to verify address or port numbers of the source and/or destination. However, most routers don't waste Filtering a lot of time ... When a packet is received with AWS Firewall Manager, threats can be reported to your safety team so they can react and mitigate an attack quickly.

Whether they receive one or thousands of packets, every package is individually treated and we don't. Maintain track of packets we've seen before or not. This is known as stateless filtering.

On the other side, firewalls use state-of - the-art filtering. They keep track of all entry and exit links. Below are a few instances:

A computer on the LAN connects to a mail server on the Internet using its email client. The customer starts a three-way TCP handshake that the firewall considers•. You can implement AWS WAF guidelines on current or future AWS assets automatically, ensuring compliance with firewall regulations across the organization. A web server sits behind a firewall, a busy server that accepts 20 fresh TCP connections per second from separate IP addresses on average. The firewall keeps track of all links, once it sees a source IP address demanding more than 10 fresh TCP contacts Any traffic from that source IP address will be dropped per second, preventing a Do's (Service Denial).

4.1.3 Security Zones

If they have a corresponding path in their routing table, Cisco routers will allow and forward all packets they receive by default. You need to configure some access lists if you want to limit this. Users who alter their safety settings for Internet Explorer could allow hazardous Internet code kinds and websites mentioned in the Restricted Sites area of the browser to be executed

The above Router has two entry lists to prevent the traffic of some hosts. We also have two access lists that stop Internet Traffic from our network's entry. Some of the lists of access may be reusable, but we must apply an access list to four interfaces. Firewalls work with safety areas, there's a better option. Here's an instance. Security Zones is shown in fig 4.2

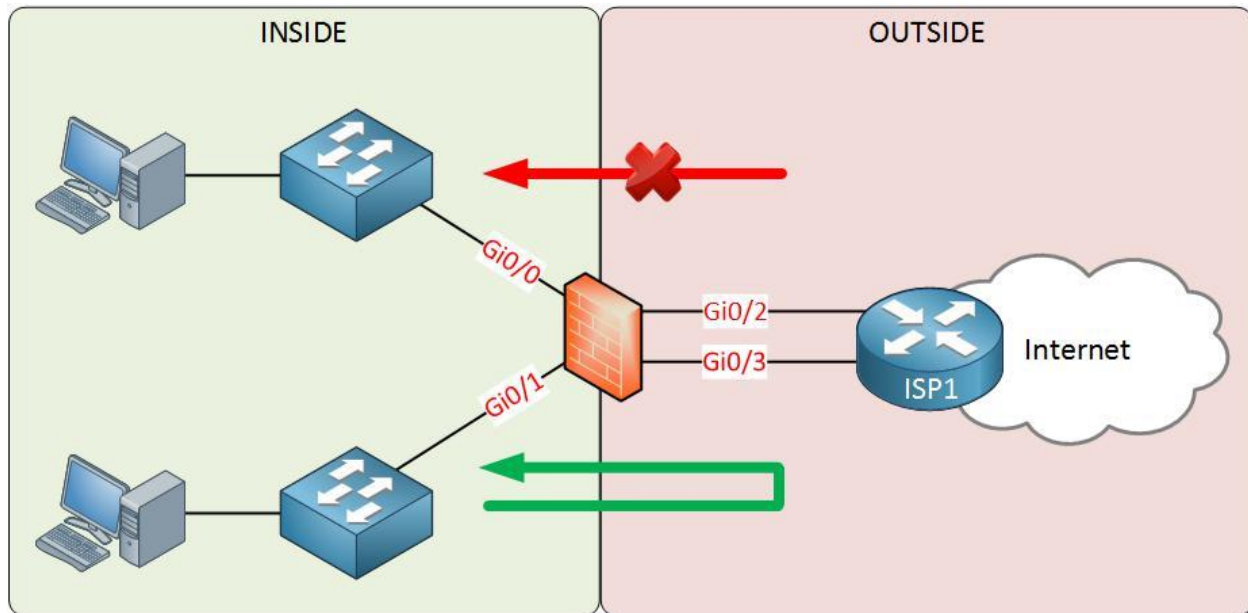


Figure: 4.2 Security Zones

4.1.4 Cisco ASA Security Levels

The Cisco ASA Firewall utilizes so-called "safety levels" to show how an interface is compared to another interface with confidence. The greater the level of safety, the more confident the interface will be. Each interface on the ASA is a security zone, so we have distinct levels of confidence for our safety areas by using these safety levels. Network Design 3 and Firewall Design Press next to continue shown in fig 4.3 & 4.4

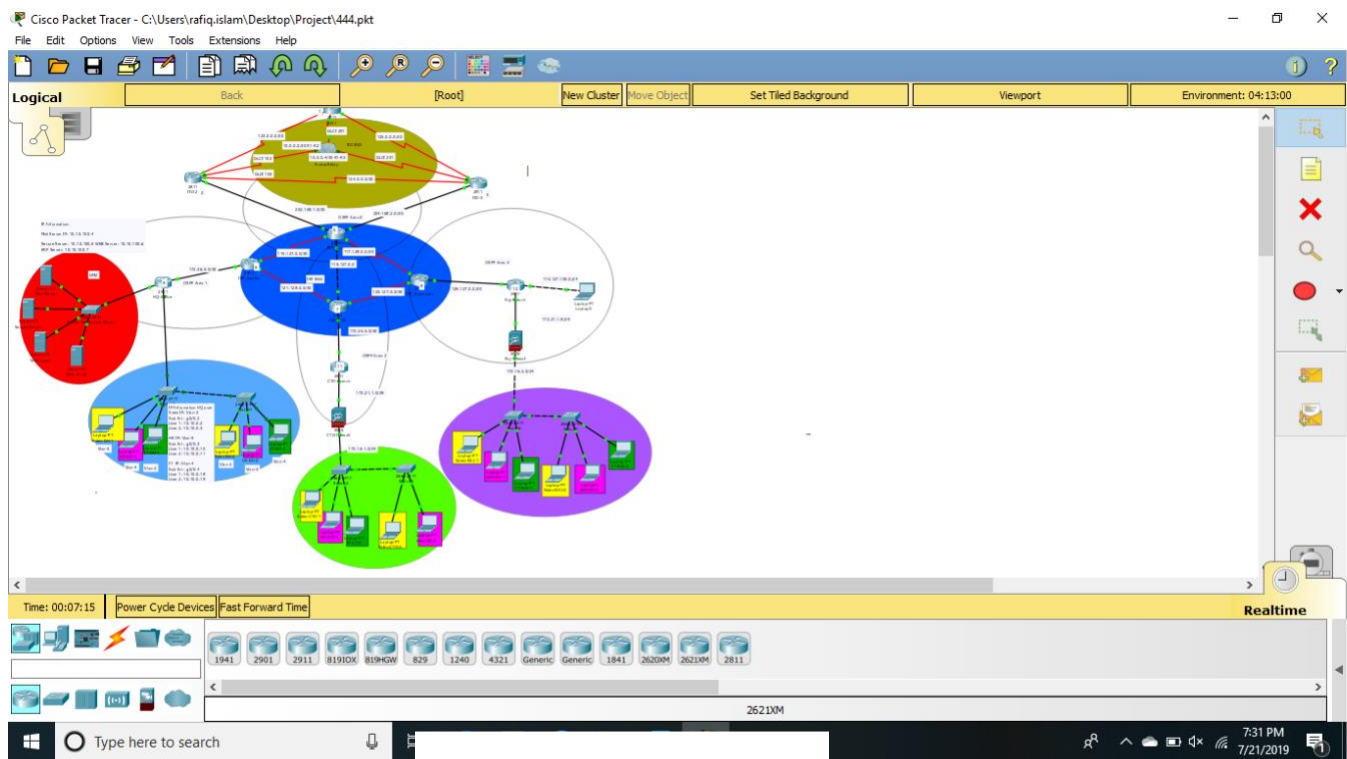


Figure: 4.3 Network Design 3

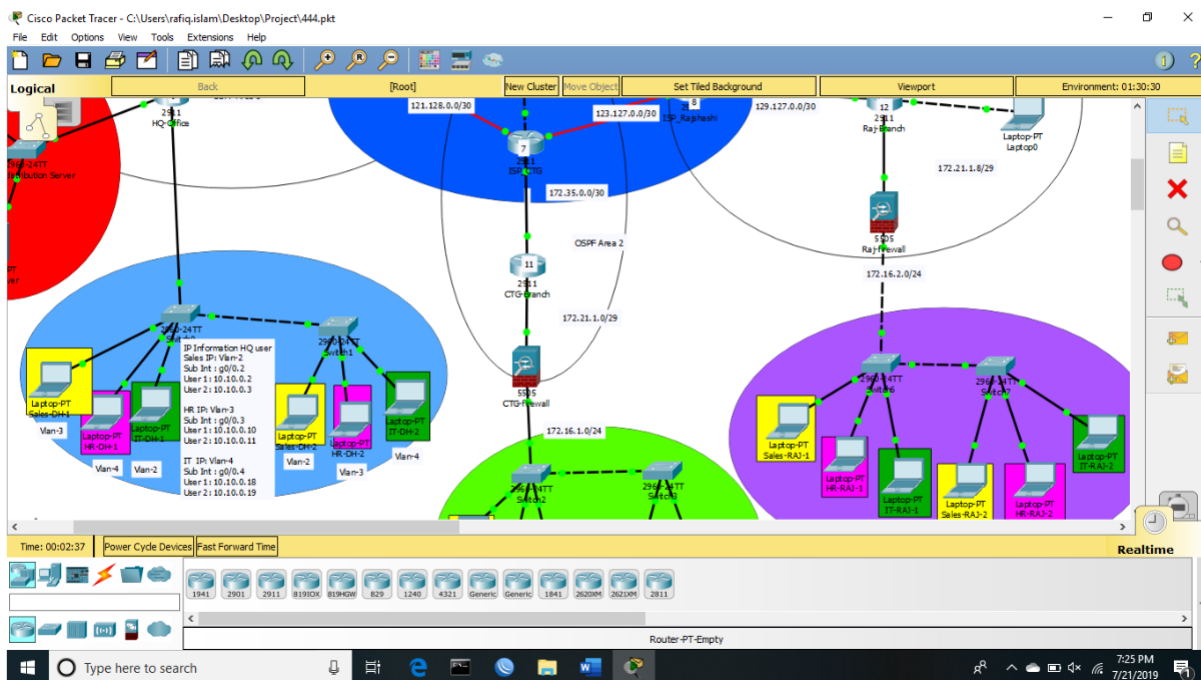


Figure: 4.4 Firewall Design

Chapter 5

Conclusion and Future Works

5.1 Discussion and Conclusion

Survey of this internship was a wonderful and rewarding background. I've seen the future and I'm going to be able to get in touch with many people and have the ability to affirm that. Through this internship, I found that one of the main problems and time management skills, as well as self-inspiration. I was eight hours a day when I first started, six days seven days will be ready to sit in an office and I didn't think that. When I understood what I needed to do my covering hours is not breached, so I arrange my ordinary day-to-day worksite. Out and it was the right moment when I got a academic response organized for questions. For a long time, I had to figure out how to propel myself through this internship and on - the-job time management.

5.2 Scope for Further Career

The analysis of the overall performances of network system of multiple of branch is not easy. It is a study on the operation and management of the office. So the report was completed under base on collecting information certain constraints which were:

- Non-availability of the pertinent information.
- Available information could not be verified. In most cases, we simply did not have any option but to finish with the information without verification.
- Due to time restrictions, the report is concentrated in selected areas only.
- Our system needs more devices and more configurations.
- Server increase more cost

5.3 Future Development

Under Linux, career possibilities are available in multiple areas. The profession opens in Linux, not just on the level of Linux, it includes portion of different areas such as: development of desktop applications, Development of the kernel and device drivers today their huge application for open source programming and the developers and system engineers of open source programming. Today, many organizations have moved to Linux and the open source software. The organization such Just like Google, Yahoo, Boeing, Lufthansa, and wiki.org .countless organizations moved to an open source agreement that was financially knowledgeable. The qualified experts in the LINUX, MICROTİK etc. have an enormous demand.

References

- [1] <https://bit.ly/32GBc5J> Access time 1/05/2019 10:23pm
- [2] https://www.webopedia.com/TERM/N/network_security.html Access time 5/06/2019 11:23pm
- [3] <https://www.quora.com/What-are-the-advantages-of-network-security> Access time 4/07/2019 9:23pm
- [4] <https://searchnetworking.techtarget.com/definition/virtual-LAN> Access time 8/07/2019 1:23pm
- [5] <https://searchsecurity.techtarget.com/definition/IPsec-Internet-Protocol-Security> Access time 5/07/2019 2:00pm

Appendix

Bank Detail:



Name	Export Import Bank of Bangladesh Limited
Address	Ring Tower, Industrial Plot No. 06/A, Ring Road, Mohammadpur, Dhaka
Telephone	02 9129421, 9129504, 017 7776340
Routing Number	100263976
Fax	02 9129341
E-mail	ringroad@eximbankbd.com
Website	www.eximbank.com