

DESIGN A NETWORK SECURITY MODEL FOR THE EXIM BANK

Submitted By

Afrin Jahan Naina

ID: 171-15-9248

A Project Report Submitted Partial compliance with the Bachelor of Science in Computer Science & Engineering requirements.

Supervised By

Saiful Islam

Professor (Senior level)

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

APPROVAL

This internship titled "**Design and Implementation of Network Security Model for Exim Bank**", submitted by Afrin Jahan Naina, ID No: 171-15-9248 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 December 5, 2019.

BOARD OF EXAMINERS



Dr. Syed Akhter Hossain
Professor and Head

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



Nazmun Nessa Moon
Assistant Professor

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

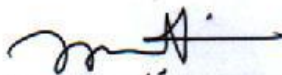
Internal Examiner



Gazi Zahirul Islam
Assistant Professor

Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Mohammad Shorif Uddin
Professor

Department of Computer Science and Engineering
Jahangirnagar University

External Examiner

DECLARATION

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

We 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:



Saiful Islam
Senior Lecturer
Department of CSE
Daffodil International University

Submitted by:



Afrin Jahan Naina
ID: 171-15-9248
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 Saiful Islam, Lecturer**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of Networking” to carry out this project. He 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	ii
Declaration	iii
Abstract	iv
Acknowledgement	v
Chapter 1: Introduction	1-4
1.1 Introduction	1
1.2 Motivation	2
1.3 Internship Objectives	3
1.4 Report Layout	4
Chapter 2: Organization	5-9
2.1 Introduction	5
2.2 Product and Market Situation	6
2.3 Target Group	7
2.4 SWOT Analysis	8
2.5 Organizational Structure	9
Chapter 3: Tasks, Projects and Activities	10-14
3.1 Daily Task and Activities	10
3.2 IP sec Protocol	11
3.3 Secure shell	12
3.4 Open shortest path first	13
Chapter 4: Competencies and Smart Plan	15-19
4.1 Competencies Earned	16
4.2 Tasteful Filtering	17
4.3 Security Zones	18

Chapter 5: Conclusion and Future Career	20-20
5.1 Discussion and Conclusion	20
5.2 Scope for Further Career	20

List Of Figures

Figures		Pages
Figures	2.1.1 Flow chart of connectivity of server	5
Figures	2.3.1:VLAN Configure of code	6
Figures	2.4.1 Flow Chart of Proposed VLAN	7
Figures	2.6.1:Flow chart of Proposed Network Diagram	9
Figures	3.6.1:OSPF	12
Figures	3.6.2:Switching Packet	14
Figures	4.1.1:Firewall	15
Figures	4.3.1:Security Zones	16
Figures	4.4.1 Network Design	17
Figures	4.4.2:Firewall Design	18

I

CHAPTER 01

Insertion

1.1 Insertion

Local and local security networks are now linked to the computer network. The threats to knowledge and networking have dramatically increased. Many of these threats have become clever attacks that cause harm or theft. There is an exponential Internet. As the government becomes more interested in business-critical Internet applications, there are more Immediate advantages. Nevertheless, these network-based approaches apps and services can pose security risks corporate and government data resources for citizens. Without sufficient network security and protection, most companies and Governments are likely to lose this asset. Network security is the very method used to secure digital data resources , privacy protection and availability are the most important security objectives. With this in mind, to optimize a company's value, it is important to ensure that all networks are secure from threats and vulnerabilities.

1.2 Motivation

In order to optimize the value of a company, it is necessary to safeguard all networks against threats and vulnerabilities. Two rakings that include protecting the computer network's infrastructure. Network security is an entity's strategy which maintains network security of its resources, including all network traffic Network security is usually handled by a network administrator or system administrator implementing security policy, Network software and hardware to secure open network and resource policies from unauthorized access and to ensure adequate network access and network resource access. Digitization has converted our world. All has changed our way of living, working, playing and learning. Any organization that wants to provide the services that customers and staff require must protect its network. Network security also helps to prevent proprietary data from being targeted. Basically, it preserves your image.

1.3 Internship Objective

Business computer networks are facing fresh daily threats such as spyware, ransomware, and hacker intrusions it is more IMPORTANT than ever to protect your business network before the cannot ignore the need for network security. With A network security framework, all records, data and private information are protected from unauthorized access. Individuals on the network and outside the network. It is therefore widely used in schools, Banks and many other security networks regulations and policies to protect the network Administrator controls the abuse, alteration or Some form of computer network unauthorized access. The prevention of a number of cyber-attacks and other disruptive behaviors.

1.4 Report Layout

Weaknesses: Three common words used when addressing safety of the network are vulnerability, risk, and attack Any network inherent or system, vulnerability is a weakness It includes routers, switches, desktops, servers, and even their own devices for security. There are three major ones here.

Technological vulnerabilities: There are inherent safety limitations in computer and network technology. These include TCP / IP protocol bugs, operating system defects, and network equipment weaknesses.

Configuration weaknesses: Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computer and network devices.

Security policy vulnerabilities: security policy weaknesses can lead to unexpected security threats. The network may pose safety risks for the network if users are not following the security policy.

Protect data: The protection of the network prevents unauthorized access as stated. A network includes some personal information, such as information about private

customers. Anyone breaking into the network could hamper this delicate data. In order to protect them, Safety of the network should be in operation.

Cyber-attack prevention: the majority of network interference comes from the cloud. Hackers are experts in this, and then there will be virus attacks. If they're sloppy, they can play with lots of data in the network. Network security can prevent computers from being harmed by such attacks.

Access levels: Security software provides different users with unique access thresholds. The user authentication is followed by the system of authorization in which it is verified whether the user is able to access those services. You might have seen some password protected for protection inside shared files. Obviously, the code knows who has access to funds.

Centrally controlled: Unlike computer security software, network manager is a key customer who controls network security technologies while the latter is vulnerable to worms and virus attacks, the latter can prevent hackers from harming something before doing anything.

Lower costs: It is more cost-effective to use a controlled security service than to charge IT consultants hourly and to have full-time staff. Lower spending means better performance and greater ability to pass on these benefits to your customers.

Reduced Stress: With Network Security, you will never lose sleep over worrying your company's security. We'll handle everything so you don't have to be safe now you have more time to focus on making your business even more successful because you know it's for security purposes. In this tip, we will investigate why these devices are simple targets, how many of today's malicious network assaults on routers, switches and firewalls are being carried out; and what an organization can do to defend the network against them.

Attacks

In general, some of the most common router attacks include

Denials of service attacks are most frequent (DOS): The attacker or attacker uses a number of requests to flood the networks of routers with requests for messages. Using ICMP packets, they send requests. This is the Internet Message Protocol Command. Such packets are sent from multiple locations over a short space of time.

Packet mistreating attacks attempt to insert malicious code: Packet maltreatment is the second most common router attack. To confuse and interrupt the router and network, maltreatment packets are loaded with malicious codes similar to DOS attacks. As the name of the hacking method indicates, the data packets mistreat the router, resulting in the router starting to mistreat the harmful packages within the network.

Routing table poisoning manipulates the routing table: As mentioned above, each router has something called a routing table which transfers and receives information. Unfortunately, the routing table can become extremely vulnerable without proper protection and encryption..

Hit and run attacks: Another of the most popular router attacks is a hit and run attack that is designed as a one-off assault on a particular network or router. Hit and run attacks are often called 'check hacks' and also happen when malicious information is inserted by software into the router. Typically when at their first attempt an attacker fails, they may or may not succeed and make further attempts on the process.

Chapter 2 Organization

2.1 Introduction

A server is a computer program or machine that provides a service to another computer program and its user, often known as the client. Also often referred to as a client in a data center is the actual device operating on a software system. This computer may also be a dedicated server or for other purposes.

Servers include:

- Mail servers
- Test servers

Numerous Web applications, including websites and email services, use this client-server networking model. Continue pressing next to the server connectivity chart shown in fig 2.6.

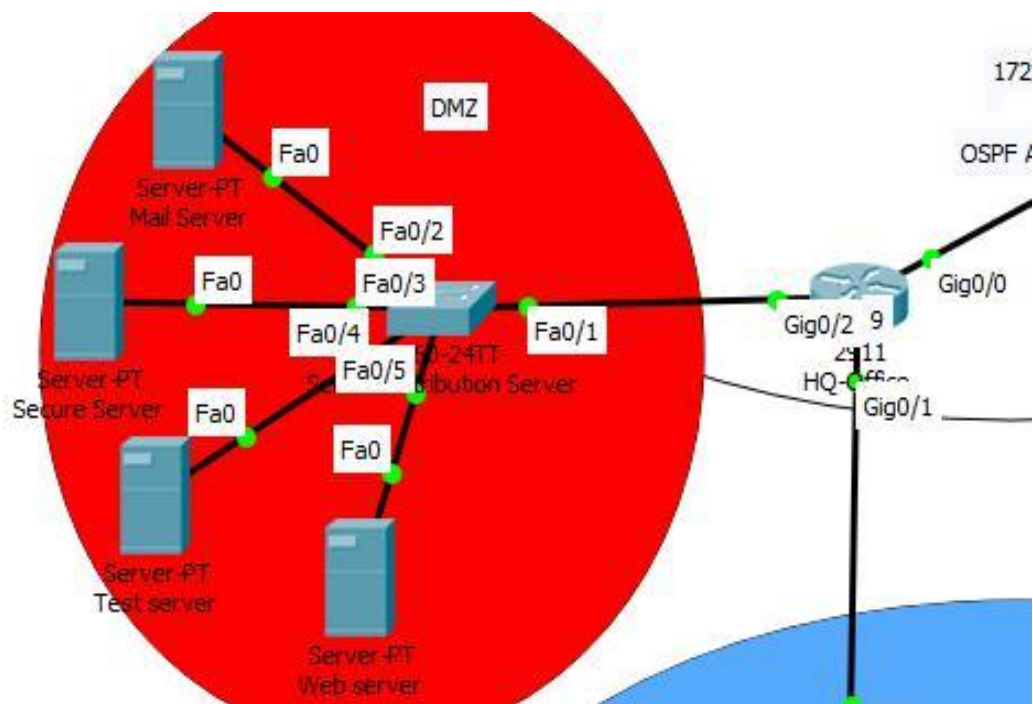


Figure: 2.1.1 Flow Chart of connectivity of server

2.2. VLAN Trunking

You can't show VLANs without considering trunks. It is understood that you can monitor and segment network transmissions with VLAN. VLAN trunking makes it possible to move traffic to different areas of the network configured as a VLAN. Most Cisco switches support IEEE 802.1Q for the synchronization of connections on Fast Ethernet and Gigabit Ethernet.

2.3 VLAN Trunk port configuration

Trunks are often used for switches and other network devices, such as a router, another switch, or a server. The design and proper functioning of a trunk must be understood to a network engineer.

```
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
  .
```

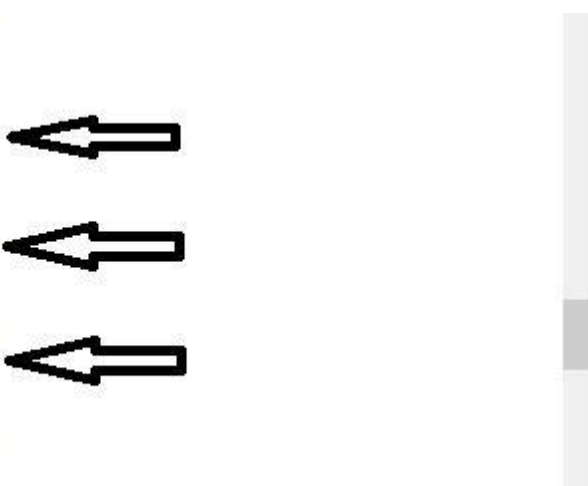


Figure: 2.3.2 VLAN Configure

2.4 Flow Chart of Proposed VLAN

Continue pressing shown in fig 2.4.3

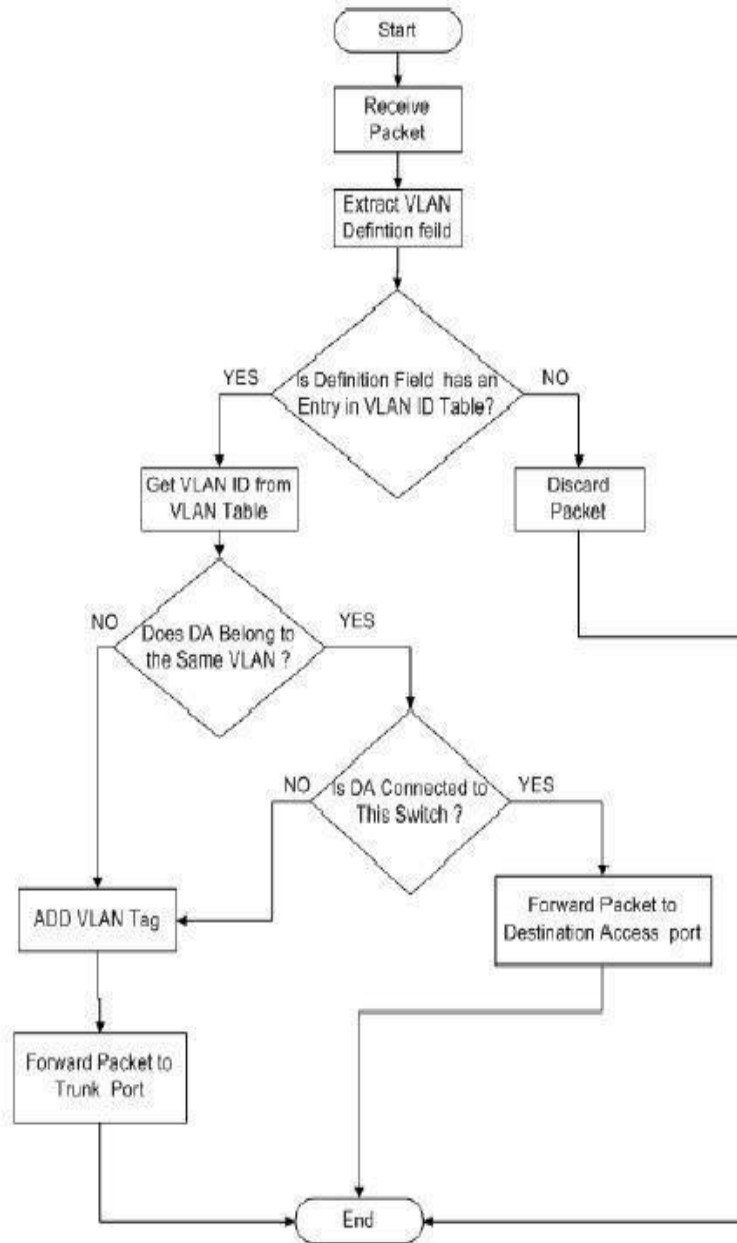


Figure: 2.4.1Flow Chart of proposed VLAN

2.5 Variable Length Subnet Mask (VLSM):

VLSM, subnetworks use the necessary block size to require different subletting. Suppose an administrator is in charge of managing four departments. These are sales and purchase department with 120 pcs, development department with 50 pcs, account department with 26 pcs and leadership department with 5 PSC.

1 This can provide complete protection for VTYs by removing all non-IP remote access to use SSH and IP Security Encryption (IPsec) all wireless router connections instead of TELNET. Remote monitoring is inherently dangerous because the router passwords can be obtained by anyone with a network sniffer on the wrong LAN segment and then taken over the router.

2 Applied routing access control lists, malicious traffic packets filtering and tariff limits, this filtering can usually be carried out on the basis of two networks.

3. The routing of access control lists will limit all traffic to internal network IP addresses which are not part of internal networks, Accept all existing network traffic with an internal origin address and accept all traffic with an address source or destination reserved, uncountable or unlawful.

4. In addition, configure Authentication Proxy to use AAA to Set up an authentication account for router and firewall, local area server and authentication. This is the new access control facility for Cisco to manage access, permissions and customer actions on a router. Authentication is the method by which the user is confirmed before accessing a network object is permitted. Authorizations is the methodology used after the router has been authenticated to determine what a client has the right to do.

5. Cisco IOS firewall IDS is an IDS designed to improve boundary routers in real time. Security by identification, recording and cessation of unauthorized activity. For many, but not for all, Cisco routers, this facility is available in IOS versions. A distinctive benefit of

applying an IDS to a router, particularly a boundary router, is that it flows and can be examined across all network traffic.

6. Use the network security port on the switch to prevent assaults at the CAM table. When port protection can be implemented in three ways: fixed, secure MAC addresses, dynamic and secure MAC addresses. When a port security breach occurs, the type of action taken falls into the following three classifications: Secure, Disable, Shutdown.

2.6 Proposed Network Diagram (Our Network Design)

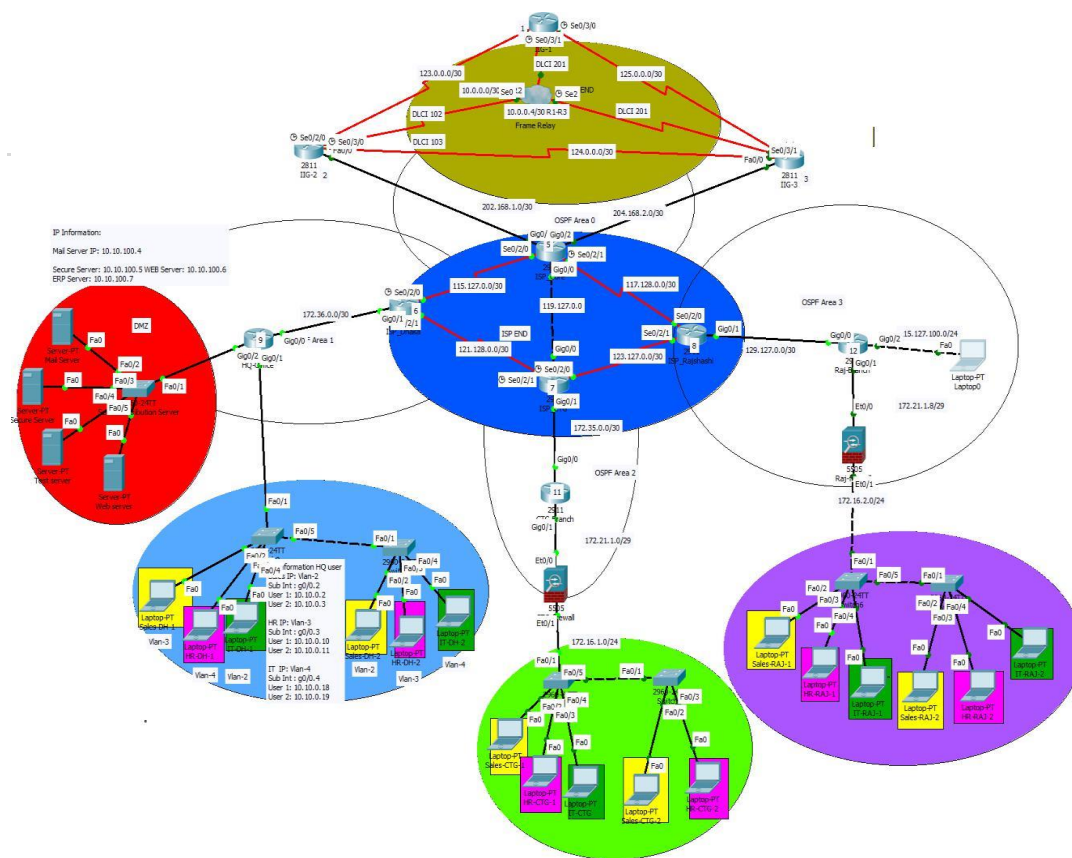


Figure: 2.2.5 Flow Chart of Proposed Network Diagram

Chapter 3

Tasks, Projects and Activities

3.1 Daily Task and Activities

With our IP Lookup Instrument, you will find your IP location. Because of many different variables, no IP Lookup tool is 100% accurate. People believe that if they are searching for an IP address, they will find the physical address given to the IP by the user. That's not true. We actually do not know of any list of IP addresses that will provide you with the exact physical location of the IP address you are searching for. At best, you'll get the exact city in which the IP client is. For a correct physical address, the IP address in question must be contacted by the ISP (Internet Service Provider).

3.2 IP sec protocols:

It is used by two moderators to safeguard an end-to-end debate. This defense only guarantees authentication. IPsec manages the IP datagram's payload only by adding a header between the IP header and the upper IP rates. The header is modified to show that the next header to be processed is the AH protocol (last header field). Except for some mutable IP header fields, the hashing mechanism is authenticated and sent to the destination. The IP datagram is entirely encapsulated in a new IP datagram using IPsec. The packet is sealed with an Integrity Check Value to authenticate the sender and avoid transit changes encapsulating the whole IP header and the IP header. The payload allows source and destination addresses to differ from the packet addresses (this allows tunneling)

3.3 Secure Shell (SSH):

The SSH protocol (also known as Secure Shell) is a technique for secure remote connection between computers. This provides many alternatives for strong authentication and preserves data protection and integrity with strong encryption. Unprotected login protocols (such as telnet, rlogin) and insecure file transfer methods (such as FTP) are a safe solution.

Open Shortest Path First (OSPF):

Open Shortest Path First (OSPF) is a connection-state routing protocol that discovers the best route between source and destination router using its own Shortest Path First. The Internet Engineering Task Force (IETF), i.e. a protocol to transfer the packet within a broad autonomous system or routing area, introduces OSPF as an Interior Gateway Protocol (IGP). It is a network layer protocol that uses the 110 AD definition of the 89 protocol. For regular contact, OSPF uses the allocated router (DR)/Backup Designated Router (BDR) multicast address 224.0.0.5 and for upgrading 224.0.0.6.

This helps the network to send and receive IP packets depending on the price of the link bandwidth via the shortest path between source and destination. OSF Press next to continue shown in fig 3.1

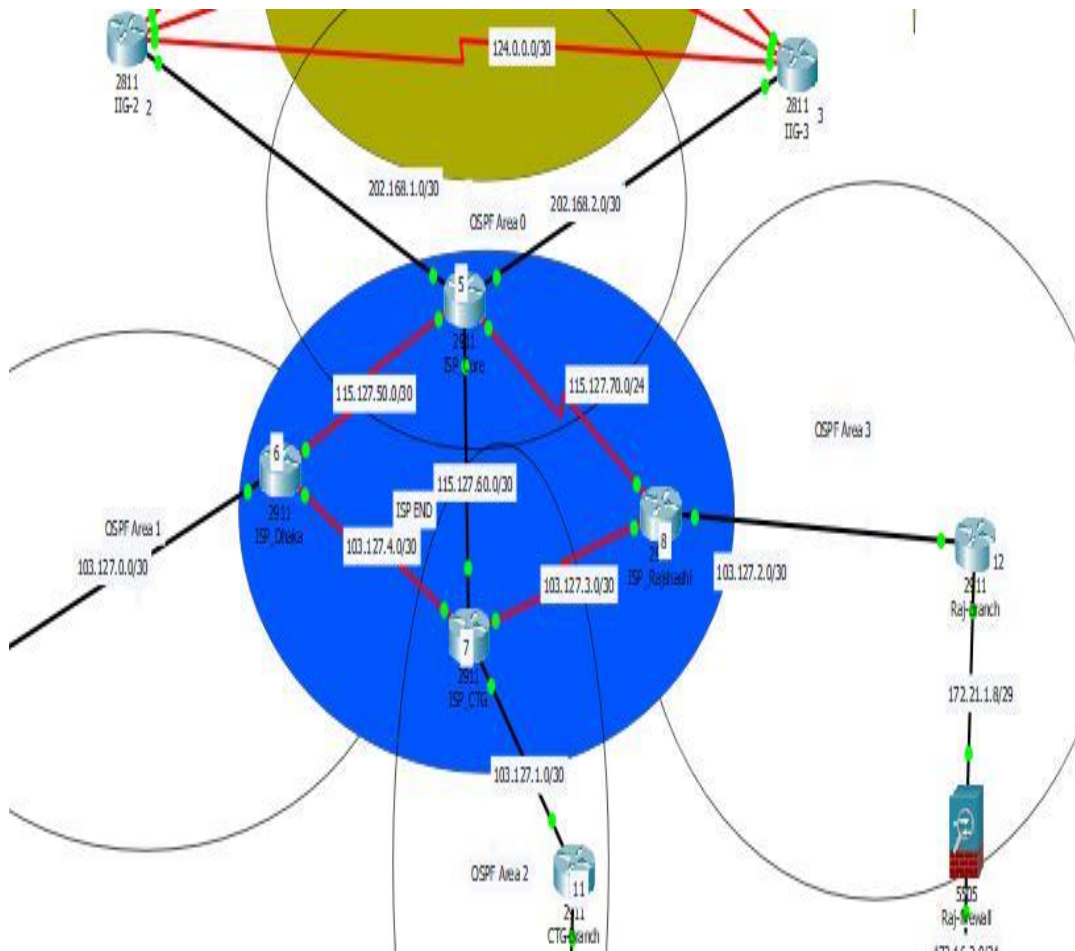


Figure: 3.6.1 OSPF

Switch

Until home routers became mainstream, the devices for the Ethernet switch widely used on home networks; broadband routers integrate Ethernet switches as one of their many features directly into the system.

For High-performance corporate networks and data centers network switches are still commonly used. While switching capabilities exist for multiple network types, the most common type is the Ethernet switches. Mainstream Ethernet switches such as those inside broadband routers support Gigabit Ethernet speeds (1 GBPS), but high-performance switches such as those in data centers generally support 10 GBPS.

Different network switch designs support different connected device numbers.

Network switches of consumer standard provide four or eight connections for Ethernet devices, Although usually corporate switches allow 32 to 128 connections. Additionally, switches can be connected to one another, a so-called daisy chaining process to slowly attach more devices to a LAN.

Network switches run on the OSI model's second layer (Data Link Layer).

Activities to switch:

- Incoming frame switched to one outgoing line.
- Many transmissions at same time
- Frame handling done in hardware
- Multiple data paths and can handle multiple frames at a time
- Can do cut-through
- Flat address space
- Broadcast storm
- Only one path between any 2 devices
- Solution 1: sub networks connected by routers
- Solution 2: layer 3 switching, packet-forwarding logic in hardware

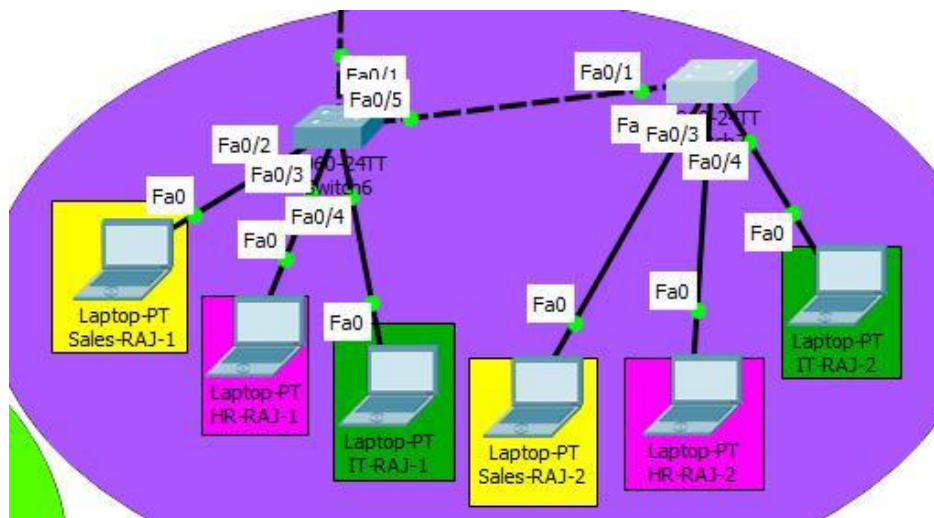


Figure:2.2.1connect switch

Chapter 4

Competencies and Smart Plan

4.1 Competencies Earned

The firewall is the barrier that is widely used between the LAN and WAN between a trusted or untrusted network. AWS Firewall Manager is a security management system that simplifies the central setup and management for your accounts and applications of AWS WAF rules. Firewall Press next to continue shown in fig 4.1

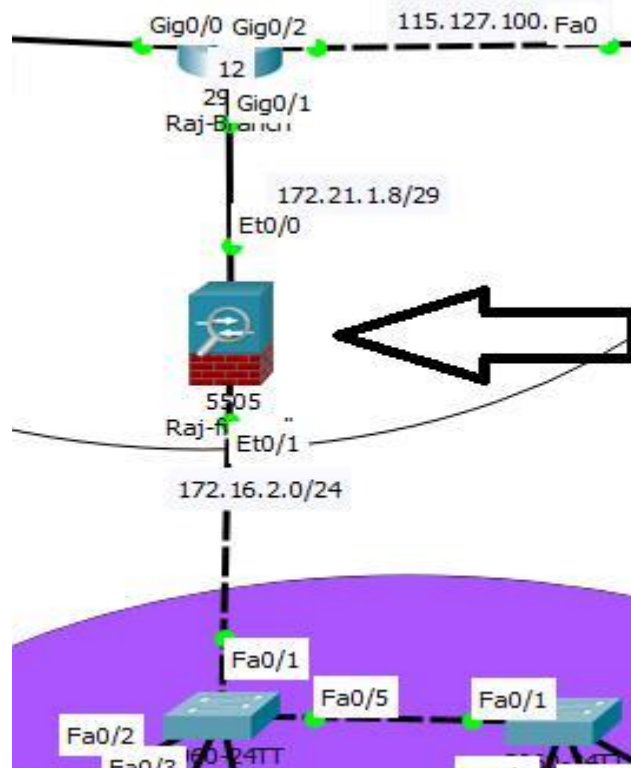


Figure: 4.1.1 Firewall

Upstairs we have a host machine and a LAN toggle. On the left, there is a router linked to the ISP that provides Internet access to secure our LAN, the firewall is in between. Depending on your WAN availability, the router is accessible, Firewall Manager also makes it easy for new applications and technologies to comply with a common set of security rules that you now have a single service to build firewall regulations, set security policies, and continuously enforce them. You'll also also need the router if you do any (advanced) routing like BGP. Some firewalls support some basic routing alternatives: static routes, default paths and sometimes routing protocols like RIP, OSPF or EIGRP.

4.2 Tasteful Filtering

Including routers, firewalls can use access lists to confirm origin and/or destination address or port numbers. But most routers don't waste a lot of time filtering. Threats can be recorded to your security team when a packet is received with AWS Firewall Manager so they can respond and mitigate an attack quickly.

Whether they receive one or thousands of shipments, they do not handle each package individually. Keep track of packets that we've seen before or not. This is referred to as stateless sorting.

Firewalls, on the other hand, use state-of - the-art filtering. They keep track of all connections to the entrance and exit. Here are a few examples:

Using its email client, a computer on the LAN links to an Internet mail server. The customer begins a TCP handshake that is considered by the firewall. You may automatically apply AWS WAF guidelines on current or future AWS resources to ensure compliance across the enterprise with firewall regulations. A web server is located behind a firewall, a busy server that accepts on average 20 new TCP connections per second from separate IP addresses. 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)

4.3 Security Zones

If the routing table contains a corresponding path, Cisco routers will allow and forward all packets they receive by default. If you want to restrict this, you need to configure those access lists. Users who change their Internet Explorer security settings may be able to execute dangerous Internet code types and websites listed in the browser's Restricted Sites zone the above router has two entry lists to prevent the traffic of certain 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 There's a better option to work with safety areas. Here's an example. Security Zones Press next to continue shown in fig 4.2

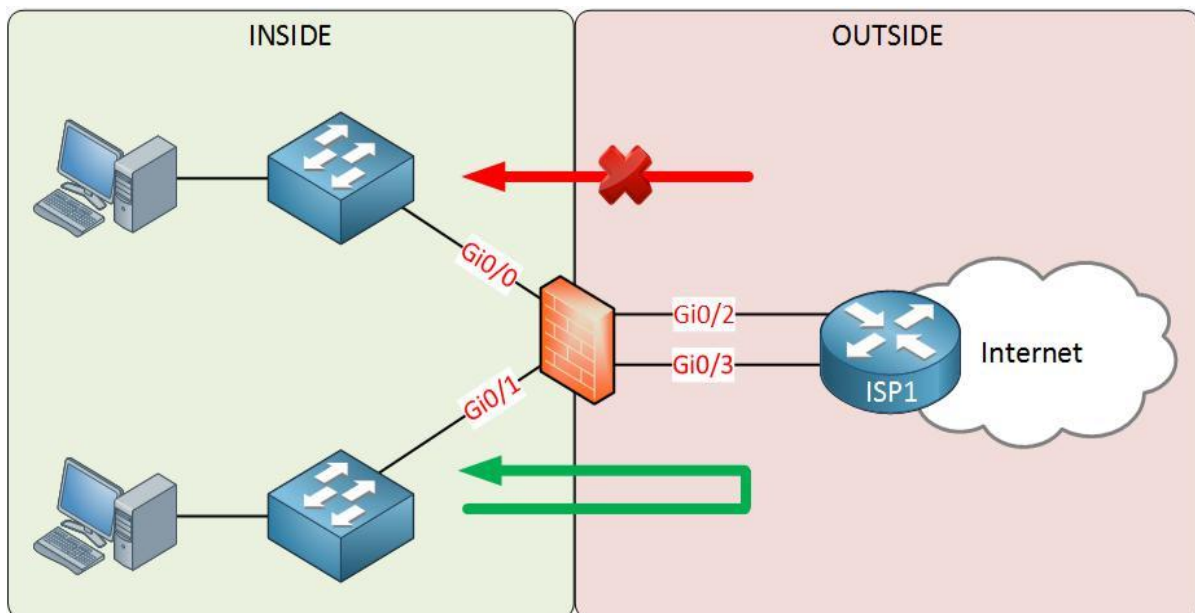


Figure: 4.3.2 Security Zones

Cisco ASA Security Levels

The Cisco ASA Firewall uses so-called "safety levels" to demonstrate how an interface is confidently compared to another interface. The higher the safety level, the more confident the interface is. Each ASA interface is a security zone, so we have different levels of confidence in our security areas by using these levels of safety. Network Design 3 and Firewall Design Press next to continue .

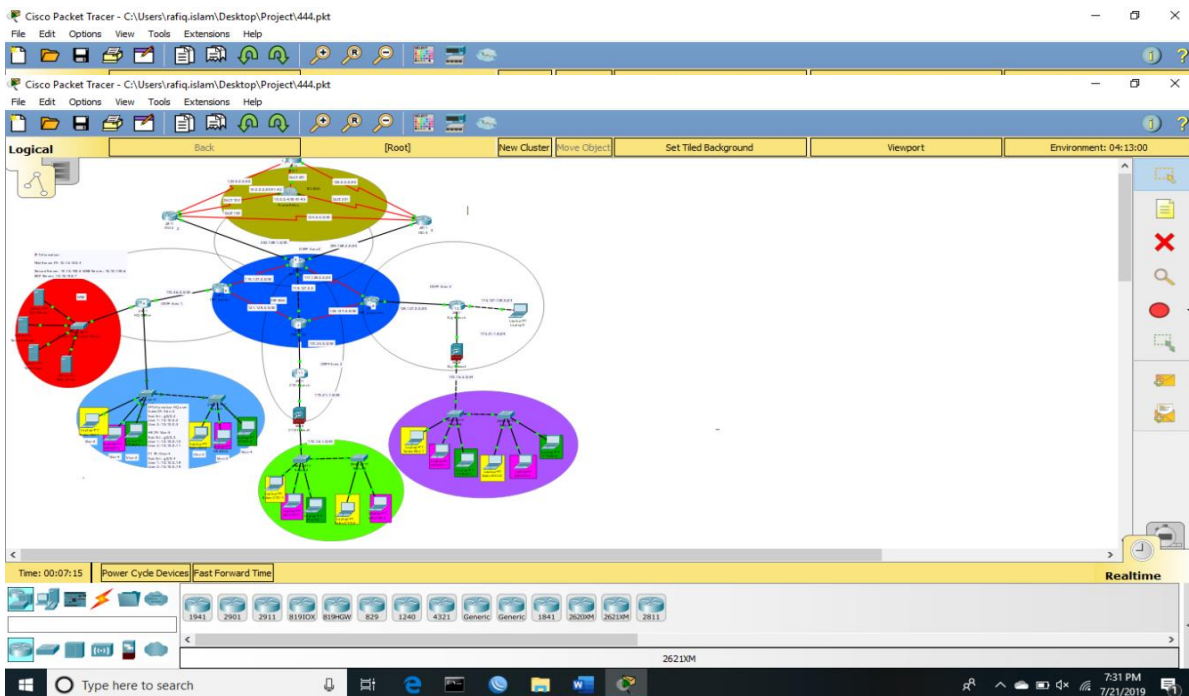


Figure: 4.4.3 Network Design

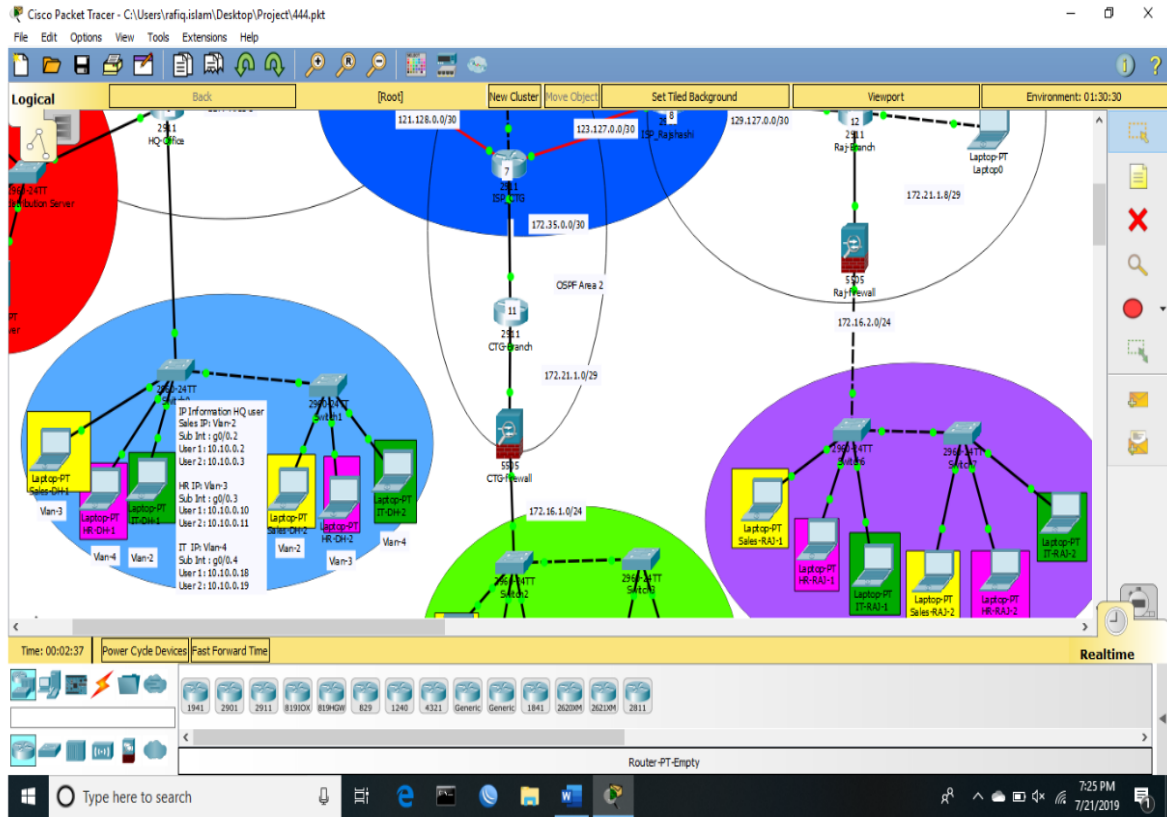


Figure: 4.4.4 Firewall Design

Chapter 5

Conclusion and Future Works

5.1 Debate and Conclusion

This internship survey was a fantastic and enjoyable history. I've seen the future and I'm going to be able to communicate and affirm that with many people. Through this internship, I noticed one of the most important issues and skills of time management, as well as self-inspiration. I was eight hours a day when I first started, seven days will be able to sit in an office for six days, and I didn't think so. When I knew I had to do my hours of shielding, my normal day-to-day job is not disrupted. Out and when I got an authoritative answer arranged for questions, it was the right moment. For a long time, through this internship and on - the-job time management, I had to find out how to move myself.

5.2 Scope for Further Career

It is not easy to analyze the overall performance of multiple branch network system. It is a review of the office's operation and management. Thus the document was completed on the basis that certain constraints were collected:

Failure to provide the relevant information.

It was not possible to verify the available information. In most cases, we simply had no choice but to complete the data without checking.

The study is focused in selected areas only because of time constraints.

More devices and more configurations are required in our system.

Server increase more cost

5.3 Future Development

The practice opens in Ubuntu, not just at the Linux level, but includes a portion of various areas, such as: Production of desktop applications, production of kernel and machine drivers, and their vast The foundation for open source software and designers for open source and application engineers. Today, several companies and open source software have switched to Linux. The company, including Google, Facebook, Airbus, Lufthansa, and wiki.org, switched to a financially competent open source agreement. The professional LINUX, MICROTIK, etc. experts have a huge demand.

References

1. Learn about Network World, available at << <https://www.networkworld.com/>>>, Last accessed on 10-09-2019 2:00pm
2. Learn about network-security available at <<<https://www.quora.com/advantages-of-network-security>>> Last accessed on 16-09-2019 4:30 pm
3. Learn about definition available at <<<https://searchnetworking.techtarget.com>>> Last accessed on 02-10-2019 8:30 pm
4. Learn about search security/IP sec available at << [/https://searchsecurity.techtarget.com](https://searchsecurity.techtarget.com) >> Last accessed on 10-10-2019 11:40 pm
5. Name: access-control-list /security available at<<<https://searchsoftwarequality.techtarget.com>>> Last accessed on 15-10-2019 3:30 pm

Bank Detail:



Name	Export Import Bank of Bangladesh Limited
Address	House#4/A,Plot#4,Road#16(Old-27) Dhanmondi ,Dhaka
Telephone	+88-02-8156216 +88-02-8156253
Routing Number	+880-2-8155970
Fax	
E-mail	dhanmondi@eximbankbd.com
Website	www.eximbank.com