

**Developing Network Security-Enhanced Model for an Enterprise Network**

**BY**

**MD MEHEDI HASAN**

**ID: 151-19-1649**

**AND**

**E-OHAB AHMED**

**ID: 151-19-1669**

**AND**

**MD.FARUK HOSSAIN**

**ID: 151-19-1714**

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Electronics and Telecommunication Engineering.

Supervised By

**MD. TASLIM AREFIN**

Associate Professor and Head

Department of ICE

Daffodil International University



**DAFFODIL INTERNATIONAL UNIVERSITY**

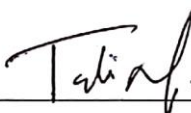
**DHAKA, BANGLADESH**

**JANUARY 2019**


## APPROVAL

This Project titled “Developing Network Security-Enhanced Model for an Enterprise Network” submitted by Md. Mehedi Hasan, E-ohab Ahmad, and Md. Faruk Hossain to the Department of Information and Communication Engineering (ICE), Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Electronics and Telecommunication Engineering and approved as to its style and contents. The presentation was held on January, 2019.

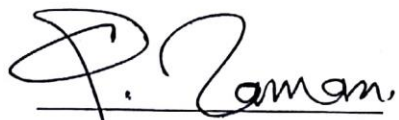
### BOARD OF EXAMINERS

  
\_\_\_\_\_  
(Mr. Md. Taslim Arefin)  
Associate Professor and Head  
Department of ICE  
Faculty of Engineering  
Daffodil International University


Chairman

  
\_\_\_\_\_  
(Prof. Dr. A.K.M. Fazlul Haque)  
Professor and Associate Dean  
Department of ICE  
Faculty of Engineering  
Daffodil International University

Internal Examiner

  
\_\_\_\_\_  
(Prof. Engr. Dr. Quamruzzaman)  
Professor  
Department of ICE  
Daffodil International University

Internal Examiner

  
\_\_\_\_\_  
(Dr. Subrata Kumar Aditya)  
Professor  
Department of EEE  
University of Dhaka

External Examiner

## DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Md. Taslim Arefin, Associate Professor, Department of ICE** 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. Taslim Arefin**  
**Associate Professor and Head**  
Department of ICE  
Daffodil International University

**Submitted by:**



**(Md Mehedi Hasan)**  
ID: 151-19-1649  
Department of ICE  
Daffodil International University



**(E-ohab Ahmed)**  
ID: 151-19-1669  
Department of ICE  
Daffodil International University



**(Md Faruk Hossain)**  
ID: 151-19-1714  
Department of ICE  
Daffodil International University

## ACKNOWLEDGEMENT

First of all we would like to express our cordial gratefulness to **Almighty ALLAH** for His kindness, for which we successfully completed our project within time and we also apologize to Him for our any kind of mistakes.

We would like to express our boundless honor and respect to our supervisor, **Md. Taslim Arefin**, Associate professor and Head, Department of Information and communication Engineering (ICE), Daffodil International University. His dedicated efforts, wise advices and keen knowledge showed the path of achievement.

We would like to thank the graduate committee Dr. A.K.M Fazlul Haque Associate Dean & Professor Department of ICE, Daffodil International University and Dr. Mohammad Quamruzzaman, Professor Department of ICE, Daffodil International University and Dr. Subrata Kumar Aditya, Professor Department of Electrical and Electronic Engineering, University of Dhaka. We also like to thank to other faculty members and the staffs of the Department of Information and communication Engineering and Faculty of Engineering, Daffodil International University.

And last but not the least we must acknowledgement with due respect the constant support and patience of our family member for completing this project report.

## ABSTRACT

Networks security plays a significant role and that seriously considered as major task when design a network. A Network administrator set different rules policy and procedure to protect the network from different type of threat like passive and active attacks from various vulnerable source. The Network must be protected from accessing unknown sources. The number of threat, attacks (Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, Aurora attacks, Malware Attack ,Port Scanning , password sniffer, IP Spoofing , Session Hijacking and Man-in-the-Middle Attacks, Cyber-attack, etc. ) increasing day by day and these attack need to identify, explore and take necessary steps for prevent it. So a firewall setup required to secure the network from malicious attacks. The Networks Securities Expert day by day Discovering strong policy and make tremendous rules for prevent those attacks.

The main aim of this project is to protect the network from vulnerabilities, threats, attacks, by performing various task and different policy (like IPsec VPN, Strong Masquerades, Port forwarding, Create trusted Zone on WAN and LAN side, etc.)

In this project, An Enhanced Network security Model for an Enterprise network has been designed and presented,, Using Firewall with various networking devices. Also, this project has been conducted the network security weakness based on its firewall along with its types of threats and responses of those malicious attacks, the method of preventing those attack form hackers to access the network. Also this project provides a Checklist to use in evaluating whether a network is adhering to best practices in network security and data confidentiality. Different software (GNS3, Metasploit, Freemeter, VMware) has been installed for analyzing security threats and attacks also Bandwidth Monitoring and deployed Strong Firewalls (Fortinet-FortiGate) for prevent these.

**Keywords:** Network Security, Threats, Firewalls, Enterprise, Network design, IPsec VPN

## TABLE OF CONTENTS

Contents	Page Number
Board of Examiners	ii
Declaration	iii
Acknowledgements	iv
Abstract	v
<b>Chapter 1 Introduction</b>	<b>1-7</b>
<b>1.1</b> Introduction	2
<b>1.2</b> Enterprise Network	3
<b>1.3</b> Motivation	6
<b>1.4</b> Aims and Objective	6
<b>1.5</b> Thesis Formation	7
<b>Chapter 2 Background of Work</b>	<b>8-28</b>
<b>2.1</b> Introduction	9
<b>2.2</b> History of Network Security	10
<b>2.3</b> Types of Attacks	11
<b>2.3.1</b> Passive Attack	11
<b>2.3.2</b> Active Attack	12
<b>2.3.3</b> Distributed Attack	13
<b>2.3.4</b> Insider Attack	13
<b>2.3.5</b> Close in Attack	13
<b>2.3.6</b> Spy Ware Attack	13
<b>2.3.7</b> Phishing Attack	13
<b>2.3.8</b> Hijack Attack	14
<b>2.3.9</b> Spoof Attack	14
<b>2.3.10</b> Password Attack	14
<b>2.3.11</b> Buffer Over Flow	15
<b>2.3.12</b> Exploit Attack	15
<b>2.4</b> Threat to Network Security	15
<b>2.4.1</b> Adware	15
<b>2.4.2</b> Backdoor Trojans	15
<b>2.4.3</b> Bluejacking	15

2.4.4	Bluesnarfing	15
2.4.5	Boot Sector viruses	16
2.4.6	Browser Hijackers	16
2.4.7	Chain Letters	16
2.4.8	Cookies	16
2.4.9	Denial of Service Attack	16
2.4.10	Document Viruses	17
2.4.11	Email Virus	17
2.4.12	Internet Virus	17
2.4.13	Mousetrapping	17
2.4.14	Obfuscated Spam	17
2.4.15	Page jacking	17
2.4.16	Parasitic Viruses	18
2.4.17	Pharming	18
2.4.18	Phishing	18
2.4.19	Aurora Attack	18
2.5	Firewall	19
2.5.1	Circuit Level Firewall	20
2.5.2	Application Level Firewall	20
2.5.3	Packet Filtering Firewall	21
2.6	Fortinate Firewall	22
2.7	Features of Firewall	24
2.7.1	Based on Features	24
2.7.1.a	Stateful Inspection Firewall	24
2.7.1.b	Application Level Gateways	25
2.7.1.c	Multilayer Inspection Firewall	26
2.7.1.d	Dynamic Firewall	26
2.7.2	Based on Uses	26
2.7.2.a	Software Firewall	26
2.7.2.b	Hardware Firewall	26
2.7.3	Based on Budgets	26
2.7.3.a	Commercial or Paid Firewall	26

2.7.3.b	Free or Open source Firewall	26
2.8	Literature Review	26
<b>Chapter 3</b>	<b>Security In an Enterprise Network</b>	<b>29-38</b>
3.1	Threats in Network Security	31
3.1.1	Unstructured Threat	31
3.1.2	Structured Threats	31
3.1.3	External Threats	31
3.1.4	Internal Threats	31
3.2	Network Security Layers	32
3.2.1	Physical Layer	32
3.2.2	Data Link layer	33
3.2.3	Network Layer	33
3.2.4	Transport Layer	33
3.2.5	Session Layer	34
3.2.6	Presentation Layer	34
3.2.7	Application Layer	34
3.3	Physical Installation Attack	35
3.4	Device Communication Attack	36
3.5	Typical Enterprise Network Security Design	36
3.5.1	Virtual Private Network (VPNs)	37
3.5.2	Firewall	37
3.5.3	Intrusion Detection & Prevention System	38
3.5.4	WAN Optimization	38
3.5.4.a	Data Protection	38
3.5.4.b	Problem Resolution	38
<b>Chapter 4</b>	<b>Problem Statement of an Enterprise Network</b>	<b>39-47</b>
4.1	Problem in Existing System	40
4.1.1	IP spoofing	41
4.1.2	Insider Intrusion	41
4.1.3	Denial of Service	41
4.1.4	No Protection Against Masquerades	42
4.1.5	Firewall Trust on Trusted Network (LAN &	42



	WAN)	
<b>4.2</b>	<b>Proposed Model for an Enterprise Network</b>	<b>43</b>
<b>4.2.1</b>	<b>Strong Authentication</b>	<b>44</b>
<b>4.2.2</b>	<b>High Data Security</b>	<b>44</b>
<b>4.2.3</b>	<b>Multilevel Protection</b>	<b>44</b>
<b>4.2.4</b>	<b>Network Traffic Encryption</b>	<b>45</b>
<b>4.2.5</b>	<b>IPsec</b>	<b>45</b>
<b>4.2.6</b>	<b>Port Forwarding</b>	<b>46</b>
<b>4.2.7</b>	<b>Internet Traffic Filtering</b>	<b>47</b>
<b>4.2.8</b>	<b>Different Web Access policy for users</b>	<b>47</b>
<b>Chapter 5</b>	<b>Implementation and Evaluation</b>	<b>48-62</b>
<b>5.1</b>	<b>Devices and Appliances</b>	<b>49</b>
<b>5.2</b>	<b>Implementation of Firewall with the integration of Different Policy</b>	<b>52</b>
<b>5.3</b>	<b>Implementing port forwarding and policy against Direct Internet Traffic</b>	<b>54</b>
<b>5.4</b>	<b>Implementation of Internet protocol security in Proposed Model.</b>	<b>56</b>
<b>5.5</b>	<b>Results</b>	<b>59</b>
<b>5.6</b>	<b>Performance Analysis and Evaluation</b>	<b>60</b>
<b>Chapter 6</b>	<b>Conclusion</b>	<b>63-65</b>
<b>6.1</b>	<b>Future Scope</b>	<b>65</b>
	<b>References</b>	<b>66</b>
	<b>Appendix</b>	<b>67</b>
	<b>Abbreviation</b>	<b>68</b>

## List of Figures

<b>Chapter</b>	<b>Contents</b>	<b>Page No</b>
<b>Chapter 1</b>		
	<b>Fig 1.1</b> Enterprise Network	5
<b>Chapter 2</b>		
	<b>Fig 2.1</b> Passive Attack	11
	<b>Fig 2.2</b> Active Attack	12
	<b>Fig 2.3</b> Distributed Attack	12
	<b>Fig 2.4</b> Spyware Attack	13
	<b>Fig 2.5</b> Phishing Attack	14
	<b>Fig 2.6</b> Hijack Attack	14
	<b>Fig 2.7</b> Aurora Operations	19
	<b>Fig 2.8</b> Packet Filtering Firewall	21
	<b>Fig 2.9</b> The Working Process of Fortinate Firewall	23
	<b>Fig 2.10</b> Authentication and Security Process of Fortinate Firewall	23
	<b>Fig 2.11</b> Physical View of fortunate Firewall	24
	<b>Fig 2.12</b> Unit Operation of Fortinate-FortiGate Firewall	24
<b>Chapter 3</b>		
	<b>Fig 3.1</b> Network Security Layers	32
	<b>Fig 3.2</b> Security Present in the Different Kinds of Enterprise Network	36
	<b>Fig 3.3</b> Firewall	37
<b>Chapter 4</b>		
	<b>Fig 4.1</b> Existing Network Model of an Enterprise Network	41
	<b>Fig 4.2</b> Proposed Model	43
<b>Chapter 5</b>		
	<b>Fig 5.1</b> Proposed Model for an Enterprise Network	51

<b>Fig 5.2</b>	Aurora Attack take place IPS	52
<b>Fig 5.3</b>	Configuration FotiGate VM with CLI Mode	53
<b>Fig 5.4</b>	Ping Statistics of FortiGate Vm with Host PC	53
<b>Fig 5.5</b>	Port Forwarding in FortiGate Firewall	54
<b>Fig 5.6</b>	Object Creat in Fortigate Firewall	55
<b>Fig 5.7</b>	Policy for Direct Internet Traffic in LAN Side	55
<b>Fig 5.8</b>	Traffic History of Direct Internet Traffic Ingoing and Outgoing	56
<b>Fig 5.9</b>	VPN Configuration in Local Interface for Port Forwarding in FortiGate Firewall	57
<b>Fig 5.10</b>	IPsec VPN Configuration in Both	58
<b>Fig 5.11</b>	Firewall Policy for IPsec VPN	58
<b>Fig 5.12</b>	Lunching Aurora in Metasploit Tools with Port Forwarding	59
<b>Fig 5.13</b>	Vulnerability Scan log in FortiGate Firewall	60
<b>Fig 5.14</b>	Log Monitoring in the Firebase of FortiGate	60
<b>Fig 5.15</b>	Utilization of Bandwidth Before Applying the Proposed Model	61
<b>Fig 5.16</b>	Utilization of Bandwidth After Using Firewall	61
<b>Fig 5.17</b>	Existing System	62
<b>Fig 5.18</b>	Compression Between Existing and Proposed System	62

## **List of Tables**

<b>Chapter</b>	<b>Contents</b>	<b>Page No</b>
<b>Chapter 3</b>		
<b>Table 3.1</b>	OSI layers Attacks	35
<b>Chapter 5</b>		
<b>Table 5.1</b>	List of Tools and Device for Implementation and Application	51

**CHAPTER 1**  
**INTRODUCTION**

## 1.1 Introduction

Now, in this modern world computer network system increases rapidly day by day. Therefore a strong security system is very much important to protect the network. In a computer network, users confront dangers from a wide range of assault from hackers. So, the development of network systems and the Internet, the dangers of data and systems have risen significantly. A large number of these dangers have turned out to be cunningly practiced assaults causing harm or submitting robbery. As personal, government and business basic applications turn out to be more pervasive on the Internet, there are numerous prompt advantages. Though these network based applications can make security dangers to the users and also companies and government.

In a network system, there are many kinds of method of attacks and these are the active attack, passive attack, distributed attack, spyware attack, phishing attack, hijack attack, spoof attack, buffer overflow, exploit attack and many more. By reducing these attack a home or little office may just require fundamental security while vast organizations may require high upkeep and propelled software and hardware to keep malicious assaults from hacking and spamming. New Threats Demand New Strategies as the system is the way to your association for both real clients and would-be assailants.

Without palatable network security, various individuals, associations, and governments are in risk of losing that advantage. Network security is the method by which computerized data assets are guaranteed, the goals of security are to ensure secrecy, look after trustworthiness, and guarantee accessibility. Considering this, it is basic that all systems be shielded from dangers furthermore, vulnerabilities all together for a business to accomplish its fullest potential. Regularly, these dangers are relentless because of vulnerabilities, which can emerge from misarranged hardware or software, poor network plan, intrinsic technology weakness, or end-client indiscretion. A router is like numerous PC's in that it has numerous default service. Many of this service is useless and also used by an assailant for gathering information. For this purpose, all pointless service should be restricted in the router configuration to keep the assailant from stealing data or harm the network. In this paper, an audit of assaults on routers and in what manner can anticipate, and

alleviating it will be depicted routers and firewall are extremely basic parts of network tasks and network security. Diligent administration and careful review of switch and firewall tasks, can minimize arrange downtime, enhance security, obstruct the attacks and hackers, organize dangers decline, and help in the investigation of suspected security violation.

## **1.2 Enterprise Network**

An enterprise network is a network which helps to connect partners PCs and related contraptions across over workplaces and work bunch systems. An enterprise network diminishes correspondence traditions, empowering structure, and gadget interoperability, and furthermore improved interior and outside enterprise data management. This venture also called a corporate network.

The main motivation of an enterprise network is to extract different client and workgroups. All method should be able to contact with each other and provide and recover data. Also, physical process and gadgets ought to have the capacity to keep up and give good execution, unwavering quality, and security. Enterprise computing models are produced for this reason, encouraging the investigation and enhancement of built up big enterprise communication protocols and methodologies. [1]

In degree, an enterprise network may incorporate Local and wide Area Network (LAN/WAN), contingent upon operational and departmental necessities. An enterprise network can fuse all procedure, including Windows and Apple workstation and working frameworks (OS), UNIX frameworks, centralized computers and related gadgets like smart phones and tablets. A firmly consolidated enterprise network successfully joins and uses distinctive gadget and framework correspondence protocols. [1]

Enterprise network Includes different kind of service and server. In this service there are both public and private access. For example, web-based services could be accessed by different clients from various networks, they can also get into other services like database services. Users from Internet, internal network, and branches networks can access their e-mail and FTP accounts. For security purpose, access to database servers is restricted from internal network, it should not be obtain from public network. EN contains various networks, each network has its function, users, devices, and technology.[1]

Securing servers of the enterprise network are essential, they must be available and secure. Enterprise network has various needs, it needs availability, scalability, security, and mobility. Users at any time and from anywhere should be able to connect to services hosted at enterprise network. There are different techniques that should be implemented within the enterprise network to maintain availability. Unavailability of services damage enterprise prestige, it accommodates its business. Fast recover will avoid service unavailability, a business cannot tolerate failure, and it costs many. Various technology and mechanisms are used to defeat this shortcut, failover technology is such one. It becomes harder to maintain availability as more services are distributed in an enterprise network. Accelerated growth in an enterprise network is critical, enterprise network should be able to connect more branches networks. WAN devices such as routers should be range enough to connect new branches, we need not change the whole infrastructure of the enterprise network. In addition, enterprise network requires a scalable wireless network, so it can connect new wireless sites. Scalability permits continuation without the need to change enterprise network infrastructure.

Today most users have smartphones like android, iPhone, these phones require a wireless connection. Enterprise network should support mobility for wireless devices in order to enable mobile users to access enterprise network service from anywhere and at any time. There are different wireless technologies that can be used in an enterprise network. Wi-Fi is a wireless technology that intends to connect user inside enterprise network, they usually used for the indoor connection. It may be possible to use Wi-Fi to connect branches networks but it still limited in the distance that it covers. On the other hand, WiMAX is used to connected branches networks of large distance, it needs more equipment and devices than Wi-Fi. WiMAX connects both sites and remote users to the enterprise network. Giving a protected enterprise network is not an easy job, it needs more efforts, money, and devices. We cannot figure the enterprise network without security, it will be a big problem.



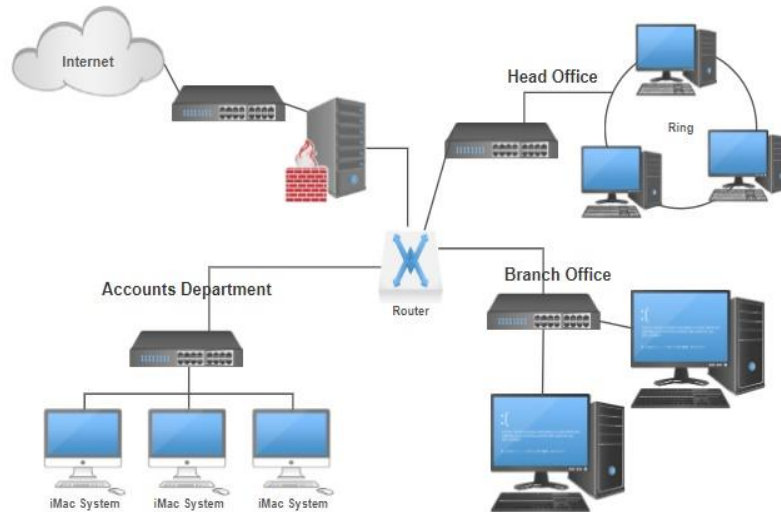


Figure 1.1: Enterprise Network

So, Enterprise network management is an important task that administrators should care about it. Analysis and collecting information from different networking devices and users necessary for monitoring and controlling EN. Most monitoring devices use SNMP protocol to collect information about network devices, they may also need to enable syslog service as well. Authors in proposed an Enhancing Enterprise Network Management using SMART, they try to make management of heterogeneous devices flexible and reliable. The paper utilized mobile agent technology for enterprise network in order to plan a hierarchical network management structure. It aims to manage 4 dynamic evolving network components using disseminated network the executives, adaptable coordination and runtime topology disclosure.

Due to the importance of Enterprise network security, we chose this topic as final year thesis to think about arrangements improving computer security. There is no total wellbeing arrangement in this way, so as to secure the data on a network, we have to develop numerous layers of insurance. A firewall is the outmost layer of the network. In this paper, we will briefly elaborate on the concept of Network security of an enterprise network, how it can be done in the past. And with the emergence and rising use of internet how security threats are pointed to our devices is also studied. The objective of this thesis is to think about the essential ideas of a firewall, dangers to computer network security, firewall topologies, how they work and organization of open source firewall items. And finally a secure network model of an enterprise network.

### **1.3 Motivation**

Usually, an enterprise network composed of a distributed infrastructure that connects different users, devices and branches networks. It includes high execution computing servers and heavy storage solutions that depend on big information, capable infrastructure, and speed network for both local area network and wide area network. Enterprise network includes data center that hosts various services such as web, E-mail, DNS, FTP, and other services. Some of these services are attained by the public user via the Internet, while others are attained via the internal network. So deploy secure enterprise network is very much important. In this Paper, we will discover the idea of an enterprise network. Also, we will see the components of EN in more detail such as devices, operating systems, network equipment's, and others.[1]

Then we will introduce the importance of network security of an enterprise network. Improper configuration of security in an enterprise network. Also, we will explain newly deployed security model of an enterprise network. This newly deployed security model minimize threats to give better secure network. Also, this security-enhanced model can be resolved the future attack.

### **1.4 Aims and objective**

Since the improper security model of an enterprise network exists, this thesis gives an overview of the different kinds of security attack of an enterprise network and how to prevent these attack. And finally gives a properly deployed security model. The aim of this work are to publish and identify the idea of attack and threat to a computer network, to highlight various allaying techniques used to complicate threats and assaults, to outline the methodology to actualize the best security model for an enterprise network. [2]

The various type of attack and different kinds of mitigation technique are discussed in this thesis. Finally implemented a secure network which prevents those attack.

So a secure model implemented-

1. To defend vital info while as yet enabling access to the individuals who require it.
2. To ensure proper authentication need access control for resources.
3. To deploy multilevel security in order to prevent vulnerability.
4. To minimize security threat from different kinds of attack.
5. To ensure guarantee in privacy and correct access.

## **1.5 Thesis Formation**

The rest of the thesis paper is created as follows:

Chapter 2 talks about the background of work. It discusses the history of network security. Also, it discussed the different types of attack and threats of an enterprise network. In this chapter, we have talked about the overall view of a firewall.

Chapter 3 explains the different kinds of internal and external threats. It also described different threats in the OSI network model. In this chapter, we have shown a typical enterprise network model. To protect the enterprise network we have talked about VPN.

In chapter 4 we have explained the existing network model of our enterprise network. We have also talked about difficulties of our network. Later we have explained our proposed security model of an enterprise network with different kinds of security-enhanced characteristics.

In chapter 5 we have implemented our proposed security model. We have use GNS3 tools to evaluate our proposed model, while we have used a FortiGate firewall to evaluate our network. We have also used a different policy to integrate our network model. Later we have discussed our result. Finally, in chapter 6, we discussed the conclusion and future work.

CHAPTER 2  
**BACKGROUND OF WORK**

## 2.1. Introduction

Network security begins with approval, ordinarily with a user name and a password. Network security comprises of the arrangements and approaches received by a network overseer to forestall and screen unapproved get to, alteration in framework, abuse, or Denial of a computer network and network available assets. Fundamentally network security includes the approval of access to data in a network, which is controlled by the network administrator. It has turned out to be increasingly critical to personal computer clients, and associations. In the event that this approved, a firewall powers to get to arrangements, for example, what administrations are permitted to be gotten to for network clients. So that to forestall unapproved access to system, this part may neglect to check possibly unsafe substance, for example, computer worms or Trojans being transmitted over the network. Anti-virus software or an Intrusion Detection System (IDS) help distinguish the malware. [1][2]

Today anomaly may likewise screen the system like wire shark traffic and might be logged for review purposes and for later on high level investigation in system. Correspondence between two hosts utilizing a network might be utilizes encryption to keep up security arrangement. The world is ending up increasingly interconnected of the Internet and new networking innovation. There is a so vast measure of individual, military, business, and government data on network administration frameworks worldwide accessible. Network security is happening to extraordinary significance in light of protected innovation that can be effortlessly obtained through the Internet. The network security is explored by researching the following:[2]

- ❖ History of network security
- ❖ Types of network attacks and security methods
- ❖ Threat to network security
- ❖ Internet architecture and security aspects of the Internet
- ❖ Security for internet access in networks
- ❖ Current development in the network security hardware and software
- ❖ Literature Review

## 2.2 History of Network Security

System and Network Technology is a key innovation for a wide assortment of utilizations. It is a basic necessity in current circumstance networks, there is a noteworthy absence of security strategies that can be effectively actualized. There exists a "correspondence gap" between the engineers of security innovation and designers of networks. Network configuration is a created procedure that is relies upon the Open Systems Interface (OSI) show. The OSI display has a few focal points when planning network security. It offers measured quality, adaptability, and institutionalization of conventions. The conventions of various layers can be effortlessly consolidated to make stacks which permit measured advancement. As opposed to secure network design is definitely not a very much created process. There isn't a system to deal with the multifaceted nature of security necessities. While considering about network security, it ought to be stressed that the entire network is secure. It doesn't just worry with the security in the computers at each finish of the correspondence chain. While exchanging starting with one node then onto the next node information the correspondence channel ought not be vulnerable to attack. A hacker will focus on the correspondence channel, get the information, and unscramble it and reinsert a copy message. In spite of the fact that anchoring the network is similarly as vital as securing the computers and scrambling the message. [3] While developing a protected system, the accompanying should be considered.

- ❖ Accessibility – Approved clients are given the way to impart to and from a specific network.
- ❖ Confidentiality – Information in the network stays private, Discloser ought not to be effortlessly conceivable.
- ❖ Authentication – Ensure the clients of the network are, the client must be the individual who they state they are.
- ❖ Integrity – Ensure the message has not been altered in travel, the substance must be same as they are sent.
- ❖ Non-repudiation – Ensure the client does not negate that he utilized the network.

### 2.3 Types of Attacks

Networks are liable to assaults from malicious sources. Furthermore, with the approach and expanding utilization of web join is most ordinarily developing on expanding. The principal classifications of Attacks can be from two classes: "Active" when a system interloper blocks information going through the system, and "Passive" in which a gatecrasher starts directions to disturb the system's ordinary activity structure must have the ability to bind hurt and recover immediately when assaults occur. There are some more kinds of attack that are additionally basic to be considered. [4]

#### 2.3.1 Passive Attack

A passive attack screens decoded traffic and scans for clear-content passwords and touchy data that can be utilized in different sorts of assaults. The checking and tuning in of the correspondence channel by unapproved aggressors are known as a passive attack. It includes traffic analysis, observing of unprotected correspondences, decoding pitifully scrambled traffic, and catching verification data, for example, passwords.

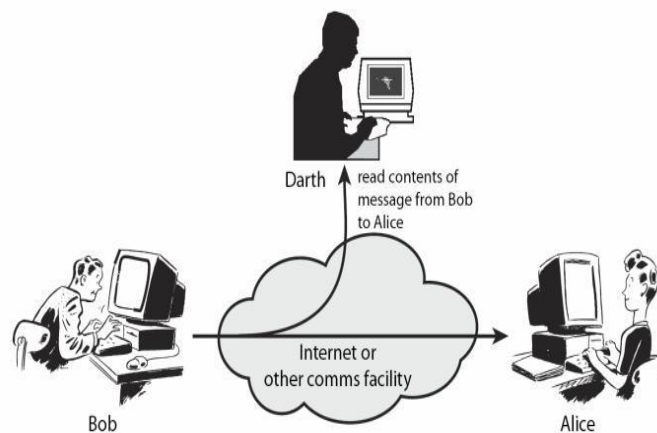


Figure 2.1: Passive Attack

#### 2.3.2 Active Attack

In an active attack, the attacker always tries to sidestep or break into secured system frameworks while the correspondence is an ongoing process. It could be done through stealth, viruses, worms, or Trojan horses. Active attack includes endeavors to break protection highlights and to take or adjust data. Unapproved attacker screens, listens to and adjusts the information stream in the correspondence channel known as a active attack.

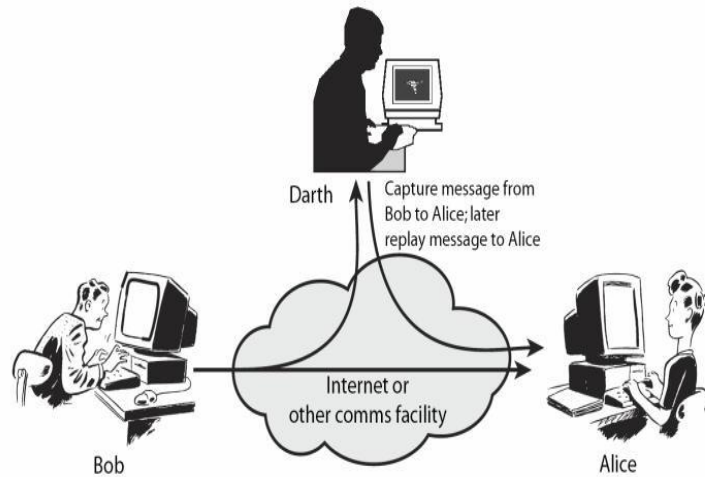


Figure 2.2: Active Attack

### 2.3.3 Distributed Attack

A distributed attack wants that the enemy present code, for example, a Trojan steed or indirect access program, to a —trusted part or programming that will later be circulated to numerous different organizations and clients. Distribution attacks center around the vindictive modification of equipment or programming at the processing plant or amid dispersion.

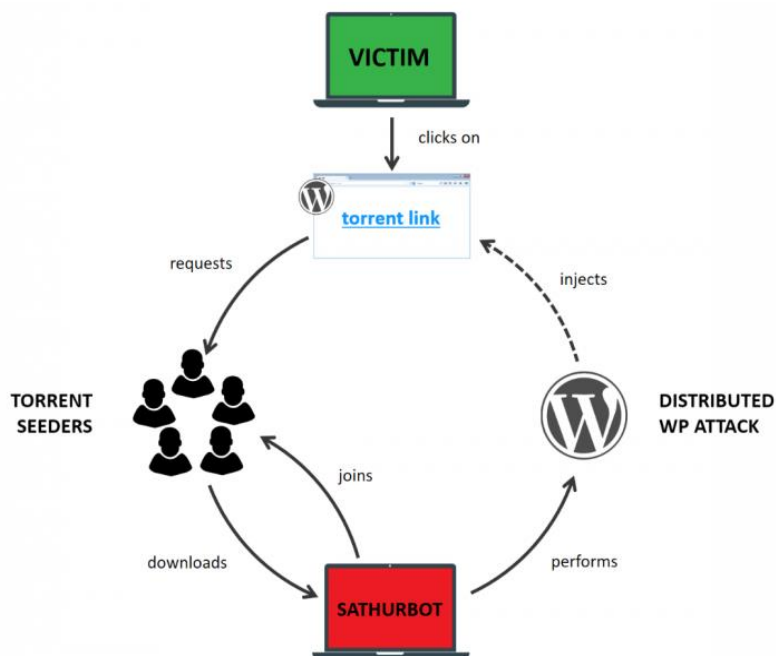


Figure 2.3: Distributed Attack



### 2.3.4 Insider Attack

As indicated by a Cyber Security Watch review insiders were observed to be the reason in 21 percent of security breaks, and a further 21 percent may have been because of the activities of insiders.

### 2.3.5 Close-in Attack

A close in attack includes somebody endeavoring to get physically near system parts, information, and frameworks so as to take in more about a system. Shut in assaults construct of standard people achieving close physical neighborhood to systems, frameworks, or offices to modify, assembling, or denying access to data. One mainstream type of close in attack assault is social engineering.

### 2.3.6 Spyware attack

Spyware is a serious computer threat that screens our online exercise or introduces a program without our assent for the benefits or to catch individual data.

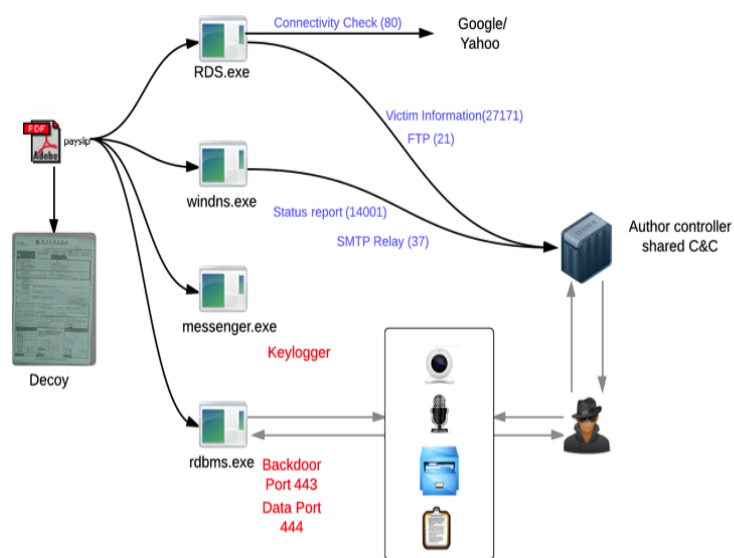


Figure 2.4: Spyware attack

### 2.3.7 Phishing Attack

Hacker creates a fake web site that looks accurately original popular site like Tweeter in phishing attack, after that Hacker send an email message and attempting to trap the client into clicking a link that lead to the fake website. When a hacker succeeds to trick a user then user tries to log into his/her account by providing account information and then hacker get the username and password after that hacker uses them on the original website.

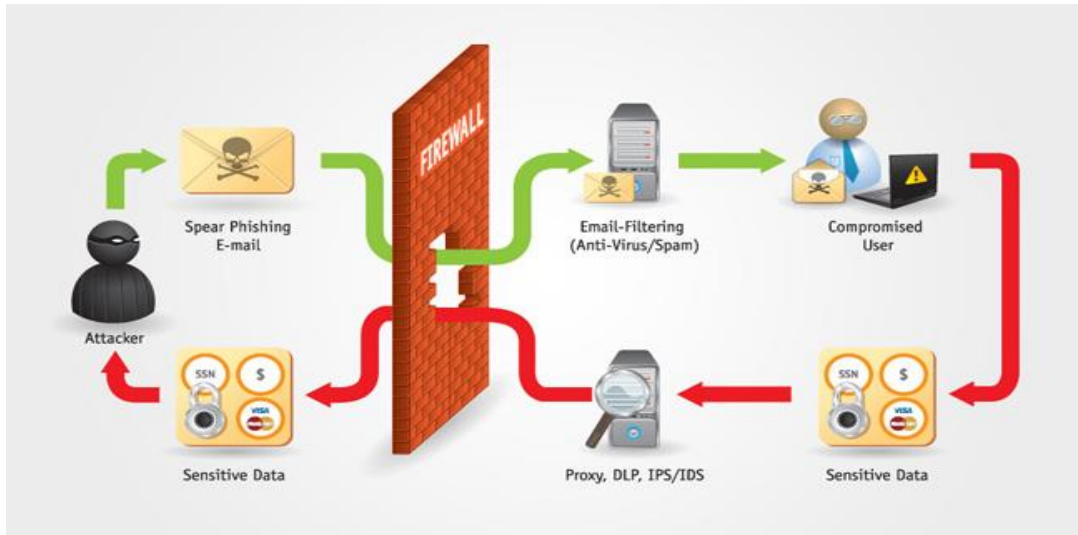


Figure 2.5: Phishing Attack

### 2.3.8 Hijack attack

In a hijack attack, a hacker assumes control over a session between two people and disconnect the other individual from the correspondence. The victims still trust that he is conversing with the first party and may send Private data to the hacker coincidentally.

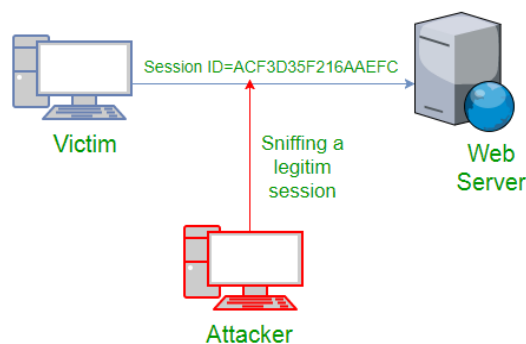


Figure 2.6: Hijack attack

### 2.3.9 Spoof attack

In the spoof attack, the attacker tone down the source address of the packets he or she is sending so that they put in an appearance to originate from another person. This might be an endeavor to sidestep the firewall rules. [4]

### 2.3.10 Password attack

An attacker endeavors to break the passwords put away in a network account database or a secret word secured document. There are three kinds of password assaults: a dictionary attack, a brute-force attack, and a hybrid attack. A word list file used on a

dictionary attack, which is a list of potential passwords. A brute-force attack is the time when the attacker attempts each conceivable mix of characters.

### **2.3.11 Buffer Overflow**

A buffer overflow attack is the point at which the attacker sends more data to an application than it is normal. A buffer overflow attack usually results in the attacker increasing managerial access to the network in an order incite or shell.

### **2.3.12 Exploit attack**

In this sort of attack, the assailants aware of a security issue inside a operating system or a bit of software and use that information by abusing the vulnerability.

## **2.4 Threat to Network Security**

There is different type of network threats discussed below...

### **2.4.1 Adware**

It is software that shows commercial on our computer. Adware, or advertising-supported program, displays advertising banners or pop-ups on our computer when we use the application. Adware can back off our computers. It can also back off our internet connection by downloading advertisements.

### **2.4.2 Backdoor Trojan**

A back door Trojan enables somebody to take control of another client's computer by means of the Internet without his or her authorization. It might act like genuine programming, similarly as other Trojan steed programs do, with the goal that clients run it. On the other hand as is currently progressively regular clients may permit Trojans onto their PC by following a connection in spam mail.[4]

### **2.4.3 Bluejacking**

Sending mysterious, undesirable messages to various clients with Bluetooth-empowered cell phones or workstations is called blue jacking. Bluejacking relies upon the capacity of Bluetooth phones to recognize and contact other Bluetooth gadgets adjacent.

### **2.4.4 Bluesnarfing**

Bluesnarfing is the robbery of data from a Bluetooth phone. Like Bluejacking, Bluesnarfing relies upon the limit of Bluetooth-empowered gadgets to recognize and contact others close-by. In theory, a Bluetooth client running the correct software on their computer can find an adjacent phone, interface with it without victim

affirmation, and download victim phone book, pictures of contacts and schedule. Our cell phone's serial number can also be downloaded and used to clone the phone. [4]

#### **2.4.5 Boot sector virus**

Boot sector viruses spread by changing the program that empowers your computer to fire up. When we switch on a computer, the hardware searches for the boot sector program which is for the most part on the hard disk yet can be on a floppy disk or CD and runs it. This program by then stacks whatever is left of the working system into memory. A boot sector virus replaces the first boot section with its own, adjusted variant.

#### **2.4.6 Browser Hijacker**

Browser hijackers change the default home and inquiry pages in our Internet browser. A few websites run a content that changes the settings in our browser without our authorization. This hijacker can add easy routes to our "Top choices" organizer or, all the more genuinely, can change the page that is first shown when we open the browser.

#### **2.4.7 Chain Letters**

An electronic chain letter is an email that urges us to forward duplicates to other individuals. Chain letters, similar to virus hoaxes, rely upon us, as opposed to on computer code, to engender themselves. [4]

#### **2.4.8 Cookies**

Cookies are records on our computer that empower websites to recall your subtleties. When we visit a website, it can put a record called a cookie on our computer. This empowers the website to recollect your subtleties and track our visits. Cookies are little content documents and can't hurt our data. Be that as it may, they can trade off our privacy. Cookies can be put away on our computer without our insight or assent, and they contain data about you in a frame you can't get to effectively.

#### **2.4.9 Denial of Service (DoS)**

Denial-of-service (DoS) attack keeps clients from getting to a computer or website. In a DoS attack, a hacker endeavors to over-burden or close down a computer, with the goal that real clients can never again get to it. Typical DoS attacks target web servers and expect to make websites inaccessible. The most widely recognized sort of DoS attack includes sending more traffic to a computer than it can deal with.

#### **2.4.10 Document Viruses**

A large number of the virus is a large program that can duplicate itself and expand starting with one document then onto the next. Numerous applications, for example, word handling and spreadsheet programs, use macros.[4]

#### **2.4.11 Email Virus**

A large number of the most productive viruses disperse themselves consequently by email. Ordinarily, email-mindful infections rely upon the client double tapping on a connection. This runs the malicious code, which will at that point mail itself to other individuals from that computer.

#### **2.4.12 Internet Worms**

Worms vary from PC infections since they can engender themselves, instead of utilizing a transporter program or document. They essentially make precise of themselves and use correspondence between PCs to spread. A worm can have pernicious impacts. For instance, it might utilize influenced computers to storm websites with solicitations or information, making them crash (a "denial of service" assault). On the other hand, it can scramble a client's documents and make them unusable. In either case, organizations can be extorted.

#### **2.4.13 Mouse Trapping**

Mousetrapping keeps us from leaving a website. In the event that we can't stop with the back or close button. At times, entering another web address does not empower us to escape either. The site that mousetraps we will either not enable you to visit another address, or will open another browser window showing a similar site. A few mousetraps let us quit after various endeavors, however others don't.

#### **2.4.14 Obfuscated Spam**

Muddled spam is an email that has been camouflaged trying to trick hostile to spam software. Spammers are always endeavoring to discover approaches to adjust or disguise their messages so that our anti-spam software can't peruse them, yet we can.

#### **2.4.15 Page Jacking**

Page-jacking is the utilization of imitations of respectable web pages to get clients and divert them to different websites. Con artists duplicate pages from a setup website and put them on another site that has all the earmarks of being authentic. They enroll this new site with real search engines, so clients completing a pursuit find and pursue

Connects to it. At the point when the client touches base at the site, they are naturally diverted to an alternate site that shows publicizing or offers of various services. They may likewise search that they can't exception from the site without restarting their computers.

#### **2.4.16 Parasitic Virus**

Parasitic infections, otherwise called record infections, spread by appending themselves to programs. When we begin a program contaminated with a parasitic virus, the virus code is run. To disguise itself, the infection by then passes control back to the main program. The operating system on our computer sees the virus as a major aspect of the program we were endeavoring to run and gives it similar rights. These rights enable the virus to duplicate itself, introduce itself in memory or make changes on our computer. [4]

#### **2.4.17 Pharming**

Pharming diverts you from a genuine site to a false duplicate, enabling hoodlums to take the data you enter. Pharming misuses the manner in which that site addresses are made.

#### **2.4.18 Phishing**

Phishing is the utilization of bogus messages and websites to deceive us into providing private or individual information. Commonly, we get an email that seems to originate from a trustworthy association, for example, a bank. The email incorporates what seems, by all accounts, to be a connection to the association's website. In any case, on the off chance that we pursue the connection, we are associated with a copy of the website. Any subtleties we enter, for example, account numbers, PINs or passwords, can be stolen and utilized by the hackers who made the false site. These are few among the Network Threats. [4]

#### **2.4.19 Aurora Attack:**

There are different types of attack in Internet world whose are dangerous and Alarming for secure data form hackers and attackers. Among those attack Aurora attack is one of them. It's a cyber-attack from hacker in the real world .With cyber-attack hackers steal our valuable and essential data form us. Hackers uses different malicious tools with a false encryption that seems real and trusted. But behind that they use different algorithms and code to make false attack to hack and find out the vulnerability of a system, in aurora operations Aurora vulnerability can be allayed by

reducing the out-of-phase opening and closing of the breakers from a hackers. Some inclined suggested policy incorporate adding usefulness in defensive transfers to guarantee synchronism and including a time delay for shutting breakers. Figure 3 shows encryption of aurora attack by generating binary.

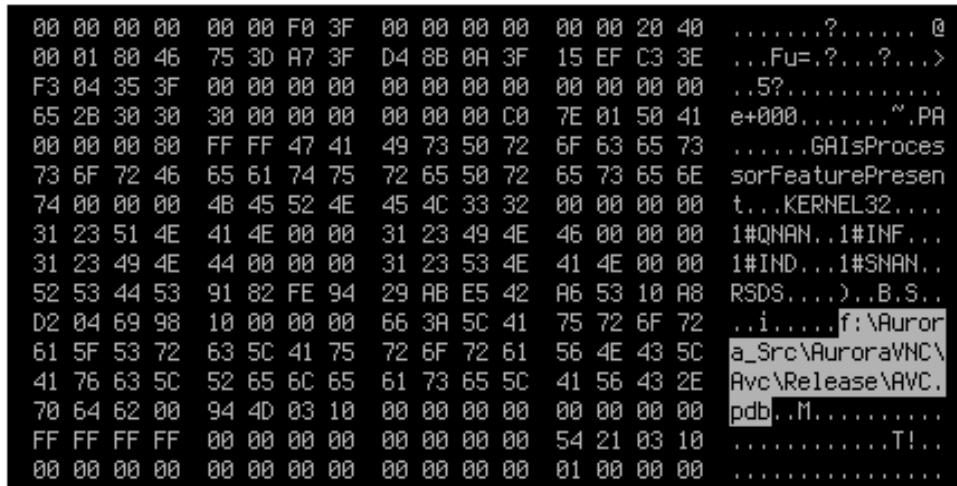


Figure 2.7: Aurora operations

## 2.5 Firewall

A firewall is a network security framework intended to keep access to or from a private network. Firewalls can be utilized as both hardware and software, or a blend of both. Be that as it may, the issue emerges when we don't know which firewall we need to utilize. So to take care of this issue we are influencing a characterization with the goal that we to can choose which firewall we have utilized by our use. Firewalls are fundamental parts of all networks. Anyway, they are hard and if not effectively configured and oversight may outcome in security breaks.

These Firewalls are the main onward edge guard component against network assaults. In any network condition network, Security is a fundamental part of network aspect and the executives. In any case, a network will commonly comprise of a wide range of client applications all of which speak to main security breaks. Besides, there are various protocols, for example, Packet assembler/disassembler (PAD), Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) that are empowered as a matter of course and should be unequivocally debilitated. While other protocol, for example, HTTP and HTTPs must be permitted yet confined utilizing access control records. It is fundamental in this way to debilitate

a conceivably extensive variety of administrations and services interfaces that are not being utilized but rather specifically limit different conventions with a proper firewall setup. Subsequent to recognizing main security branches a switch must be arranged by methods for a firewall. Firewall is a standout amongst the most generally utilized answers for the Internet world. All traffic inside to outside and the other way around must go through the firewall. Distinctive sorts of firewalls have diverse kinds of standards and operating system. The approved traffic will be sent dependent on local arrangements.[4] The firewall itself is secured, i.e.; it utilizes a confided in equipment and operating system. For the most part, firewalls are of three sorts.

- ❖ Circuit-level firewalls
- ❖ Application level firewalls
- ❖ Packet filtering firewalls

### **2.5.1 Circuit Level Firewalls**

The circuit level passage firewalls work at the session layer of the OSI model. They screen TCP handshaking between the packets to decide whether an asked for the session is authentic. And the data went through a circuit level door, to the web, seems to have originated from the circuit level gateway. Along these lines, there is no chance to get for a remote PC or a host to decide the inner private IP locations of an association, for example. This method is additionally called Network Address Translation where the private IP addresses beginning from the diverse customers inside the system are altogether mapped to people in general IP address accessible through the web access supplier and after that sent to the outside world (Internet). Along these lines, the packet is labeled with just the Public IP address (Firewall level) and the inner private IP delivers are not presented to potential interlopers. [2]

### **2.5.2 Application Level Firewalls**

An Application level passage which is additionally called a proxy server goes about as a transfer of application-level traffic. A client can contact the gateway by utilizing a TCP/IP application and afterward the gateway gets some information about the remote host which is to be gotten to. At that point accordingly the client must give a valid client ID and confirmation subtleties, at that point the passage contacts the application on the remote host and trade the TCP segments application information



between the two end focuses. Be that as it may, to play out these things the door must execute the proxy code.

### 2.5.3 Packet Filtering Firewalls

The packet sifting is done depends on the arrangement of principles configured on a packet channel router. The packet is onwards or abandoned based on the configurations done.

There are two default strategies engaged with sending or disposing of the packet, they are:

- ❖ Default: Discard (Which doesn't coordinate the arrangement of tenets)
- ❖ Default: Forward (Which becomes with at any rate any of the tenets)

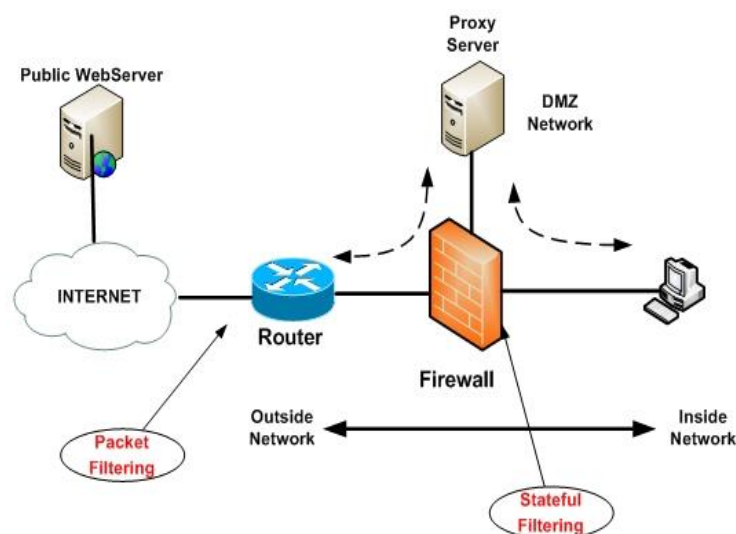


Figure 2.8: Packet filtering firewalls

In the event that a packet matches with at any rate any of the guidelines, one of the default moves makes put i.e., it is sent, and on the off chance that it doesn't coordinate with any of the arrangement of standards, at that point the other default move makes put i.e., disposes of the packet. The block diagram of a Packet filtering router is appeared in Figure 1. The packet separating is done dependent on data in the system packet. [2]

- ❖ **Source IP address:** The IP address from where the packet is produced.
- ❖ **Destination IP address:** The IP address to which it wishes to send.
- ❖ **Transport-level address of source and destination:** The applications like SNMP or telnet which are characterized by the vehicle level port (TCP or UDP).

- ❖ **IP protocol field:** Transport protocol is defined
- ❖ **Interface:** From which interface of a router the packet is begun and to which interface of a switch the packet is.

## 2.6 Fortinet Firewall

Now a days a burning question in networking security is that how to secure of in-house or enterprise network or any other platform. Then the word of firewall is comes to our mind. Fortinet is the next generation firewall as it's deployment in a big networking sector or any local large will add a tremendous security which is really a better options for enhancing security.[5]

A security architects think that how to provide major threat protection for their enterprises or any other platform including intrusion prevention, DoS attack, web filtering, anti-malware and various types of application control, will face a major complexity to hurdle managing these point products as well as no integration and lack of visibility. A prediction and Gartner estimates that by 2019 80% of enterprise traffic will be encrypted and 50% of attacks targeting enterprise will be backdoor in encrypted traffic.

FortiGate Next Generation Firewall uses reason fabricated security processors and threat knowledge security administrations from FortiGuard labs to convey top of the line assurance and elite including scrambled traffic. FortiGate decreases unpredictability with robotized deceivability into applications, clients and organize and gives security evaluations to receive security best practices.

Working procedure: A Fortinet hyper version of FortiGate which protects TCP/IP layer or other important layer. Its gives the multilayer security of network topology. Figure 2.9 shows the working procedure of Fortinet-fortiGate Firewall. Figure 2.10 shows the different steps of authentication and filtering in Fortinet firewall.[5]

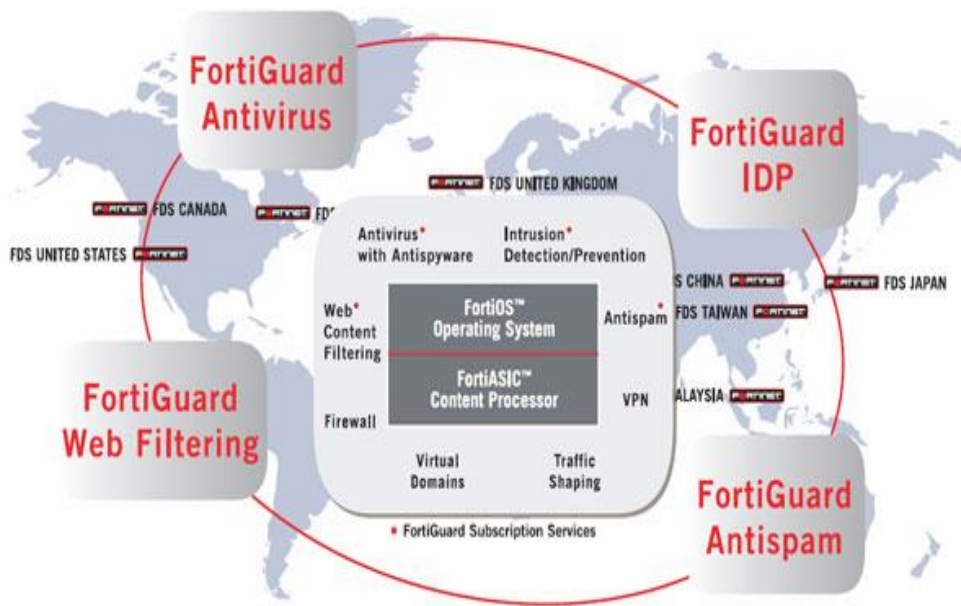


Figure 2.9: The working process of Fortinet firewall



Figure 2.10: Authentication and Security process of Fortinet firewall

Physical device of Fortinet firewall that shows below in the figure 2 (a) with different types of model and physical port. Forti analyzer will gives clear understanding about that device .figure 2(b) shows that unit operation in forti Analyzer with its port view and different potentiality. [5]



Figure 2.11: Physical view of Fortinet firewall

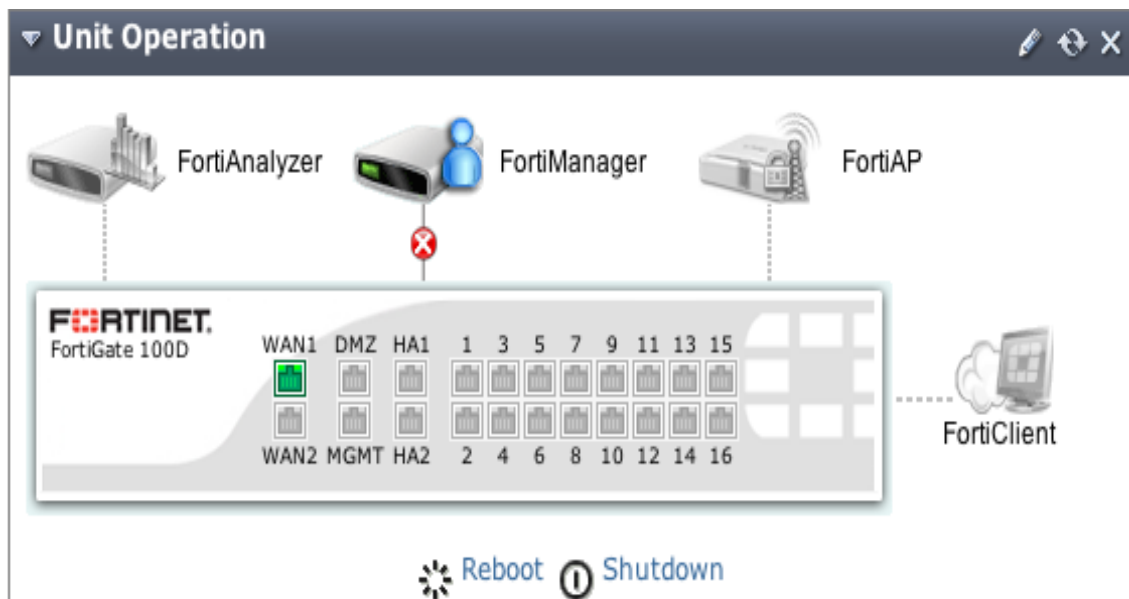


Figure 2.12: Unit operation of Fortinet- FortiGate firewall

## 2.7 Features of Firewall

- ❖ Based on Features
- ❖ Based on Usage

### 2.7.1 Based on Feature

#### 2.7.1.a Stateful inspection firewall

An innovation that controls the stream of traffic between at least two systems. SI Firewalls track the condition of sessions and dropping packets that are not part of a session permitted by a pre-characterized security approach. This is once in a while called session-level security since they keep state data for each system session and make permitted/denied choices dependent on a session state table.[6]

SI firewalls go past separate transmission control protocol (TCP) associations with include numerous such associations. Session-level firewalls bolster dynamic protocols by distinguishing port alternative guidelines in customer server correspondence and looking at future sessions against these arranged ports. For example, to follow File Transfer Protocol (FTP) sessions, the firewall reviews the control association, utilized for issuing command and arranging dynamic ports, and afterward permits in different data associations for exchanging files.

Since session level protection gives every one of the advantages of packet level insurance without the restrictions, it renders packet level security superfluous for generally organizes. [6]

### **2.7.1.b Application-level gateways (pro6-7iies)**

An application-level proxy server gives all the proxy highlights and furthermore gives broad packet examination. At the point when packets from the outside touch base at the passage, they are tested and assessed to decide if the security approach enables the bundle to go into the inside network. Not exclusively does the server assess IP addresses, it additionally takes a gander at the information in the parcels for debasement and modification.

A typical application-level passage can give proxy services to applications and conventions like Telnet, FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol), and SMTP (Simple Mail Transfer Protocol). Note that a different proxy must be introduced for every application-level administration. (A few vendors accomplish security just by not giving intermediaries to a few administrations, so be watchful in your assessment.) With proxies, security strategies can be significantly more amazing and adaptable in light of the fact that all the data in packets can be utilized by heads to compose the guidelines that decide how parcels are dealt with by the passage. It is anything but difficult to review pretty much everything that occurs on the door. You can also strip PC names to cover up inward frameworks and assess the substance of packets for propriety and security. [6]

### **2.7.1.c Multilayer inspection firewall**

The stateful multi-layer inspection (SMLI) firewall uses a sophisticated form of packet-filtering that examines all seven layers of the Open System Interconnection (OSI) model. Every packet is inspected and thought about against known conditions of a benevolent packet. While screening router firewalls only examine the packet header, SMLI firewalls examine the whole packet including the data.

### **2.7.1.d Dynamic firewall**

A dynamic packet filter is a firewall office that can screen the condition of dynamic associations and utilize this data to figure out which network data to permit through the firewall. By recording session data, for example, IP locations and port numbers, a dynamic parcel channel can actualize a lot more tightly security pose than a static bundle channel.[6]

### **2.7.2 Based on Usage**

A dynamic packet filter can actualize a lot more tightly security pose than a static bundle filter.

#### **2.7.2.a Software firewall**

It is a bit of software that is introduced on our computer so as to shield it from unapproved access.

#### **2.7.2.b Hardware firewall**

It is a gadget to which we interface with our computers or network so as to shield them from unapproved access.

### **2.7.3 a Based on budgets**

#### **2.7.3 b Commercial or paid firewall**

A firewall which possesses a fully fledged properties and any clients can utilize it however they need to pay to utilize those administrations. [6]

Examples: Cyberoam, SonicWALL-Dell

#### **2.7.3.c Free or open source firewall**

The firewall which is accessible uninhibitedly and can be utilized by anybody and anybody can change the source code and even discover bugs and report them.

Example: IPFire, IPCop, PFSense, etc.

## **2.8 Literature Review**

The comparison between the commercial and the open source firewall in an enterprise network. Also discussed and focused on the different matters by which he could make

out the difference between these two types of firewall. The proprietary firewall is better but the open source firewall can be made same as paid firewall by modifying the source code. In this paper, then we have compressively studied the features of the open source firewall which could prevent the cyber-attacks which occurs on the open source firewall in which they have made some of the rules that would prevent the entry of the outsiders in the network. So that the malicious activities inside the network could be prevented.

In this paper, the authors have concluded that for the specific instance the fortigate firewall has superior transaction rate performance and application-level filtering capabilities. The fortigste firewall is functionally superior for network-level filtering, VPN capabilities due to IPSEC, integration with a heterogeneous multi-protocol environment. We have also studied several Firewall projects in experimental stages.

At last, the best firewall arrangement might be a mix of both application level and network level packet separating. This experiment provides a basis for future experiments building toward general conclusions between open source implementations versus general commercial implementations. Effective advancement of a standard must adjust the requests of selection. Achieving the widest adoption of a standard attracts suppliers of complementary assets such as software and services, this can be achieved by widespread technology licensing on favorable terms, but by doing so, the sponsor runs the risk of losing the ability to appropriate economic rents from the standard. We described that, all main security elements of the project that were effective for its success. As we see, almost all of them were well known open source software that can be applied instead of too many proprietary and commercial tools. No product cost, free accessible updates, source code accessibility.[6]

Comprehensive method and so many other shapes can be very persuasive for entrance open source world and improve its practical and favorable software. In this paper, authors have implemented the Fortinate firewall open source firewall and then they have worked on it as a trial in organizations. In this paper, the author had defined Network's security tool was the beginning with the something that can protect the internal network from the external accessing. So, the firewall is a better perimeter defense which it enhances to provide the guard on the network's traffic. Firewall system had involved in network's environment over the years from the simple method with only packets filtering to the sophisticated packet inspectors which can decide to

allow or barrier the traffic trust on its aim, sources, and destinations. A progressive inspection packet rule is the best technology within the others firewall's technologies. It is a better or complete firewall method for a network's traffic defense.

The list of open source firewall are as follows:

- ❖ Untangle
- ❖ PFSense
- ❖ Smoothwall
- ❖ Endian
- ❖ Clear OS
- ❖ Zentyal
- ❖ IPTables
- ❖ UFW
- ❖ Vuurmuur
- ❖ ConfigServer Security Firewall

If we consider a scenario where the employee has just login its credentials and he/she is enjoying the internet services but due to some reasons like power loss, accidental removal of LAN cable/Ethernet cable from the system, or he/she has just log out from the services of using internet accidentally.[6] In such cases, the complication arises. The complications or the problem that we found in any of the open source firewall is that if any such situation arises, as the user login using its credentials the ip address of the user is stored in the firewall and the logs are generated with reference to their ip address. If the above situation arises the ip allocated to the user will return back to the pool of ip. Then the user will try to login again by providing their credentials. In such cases, the same or different ip will be allocated to the existing user. If the same ip is allocated to the user then the situation is fine. But if the different ip is allocated then the previous ip will be allocated to different user in the LAN network. As we all know that all the open source firewall provides the ip based logs. So the firewall won't be able to differentiate the actual user by taking ip into consideration. So to solve this complication/problem the logs obtained by the firewall should also have the ip address.



CHAPTER 3  
SECURITY IN AN ENTERPRISE NETWORK

## **Security in an Enterprise Network**

Securing network services and devices is the main task of the enterprise network, all data traffic is passed by network devices. We need to protect routers, switches, personal computers, servers, operating systems, and any devices in the enterprise network. Without enough protection many people's properties as well as businesses and governments are in danger of losing their riches, network security will protect loyalty, maintain fidelity, and confirm availability for an enterprise network. Enterprise network should open network security to give integrity to information data, they must be right and protected in opposition to corruption and disallowed change. Encryption provides loyalty, authenticated users can only entrance and view information data. Enterprise network includes large information that stores the heavy amount of sensitive data. Stealing of these data exposes enterprise network to compromise and even to harm business.

Enterprise network should be protected from intrusions and attacks which are originated from the internal and external network. Compromising enterprise network would be expensive, it will stop enterprise reputation which will effect on business. Enterprise network security devices should have the latest updated subscription, they should fix vulnerability of the systems, instruct traffic, and log network traffic activity. We need an updated security pattern that gleam changes in technology and services, we have to build and maintain a strong network security for end users and servers. As an enterprise network expands to include new technology, services, and systems, the likelihood of emerging new vulnerability with various degree of disability increases.

In general, security threats are arisen due to vulnerabilities, which illustrate the degree of weakness in software and hardware. Vulnerabilities are appeared due to different reasons, misconfiguration of hardware or software is a common one. Directors should avoid default configurations, they should expend more time to secure configuration. Well, network model will avoid dynamic vulnerabilities, properly allocate of network security devices is necessary through design. As new attacks arise, the challenge becomes bigger. Enterprise network should have an efficient detection and restraint system against zero-day attacks. Intrusions try to steal data of EN, they intend to compromise EN. Today attack becomes complicated, they depend on the attacker

with high skills. APT-based attacks become a serious attack against EN, they are funded by governments and organizations. They illustrate cyber-attack that want special awareness and early alerts. There are various types of APT-based attacks, Aurora operation and RSA attack are general examples. Security threats are produce from various sources, the internet is the most common one. Attacks use malicious code to compromise victim host and hence distributed across enterprise network to compromise the whole enterprise network.

### **3.1 Threats in Network Security**

The threats in network security can be divided into four sections and those classifications are the explanation of different threat occurs in a network and harmful for the whole system.

#### **3.1.1 Unstructured Threat**

The unstructured security danger is the sort of risk worked by an untalented individual peoples attempting to access a system. They usually utilize general hacking instruments, as shell contents, and secret key saltines. A legitimate security arrangement ought to effectively cross this sort of assault. At the end of the day, these type of Hackers or attackers couldn't be thought little of on the grounds that they can cause genuine damage to the system.

#### **3.1.2 Structured Threat**

In contrast to unstructured dangers, organized risk by hackers are all around gauged and profoundly adulterated. They utilize modern hacking instruments to enter systems and they can interim into government or business PCs to quintessence data. On certain reason, organized dangers are completed by epitomized criminal possess or industry contenders.

#### **3.1.3 External Threats**

Some refused individuals outsider of the organization who don't have access to the organization's PC framework or system could cause intriguing danger. They more often than not interim into the organization's system by means of the Internet or server. Both master and unpracticed programmers could present outlandish dangers.

#### **3.1.4 Internal Threats**

This kind of risk could be by a freaky worker who has approved enter to the organization's system. Like developed dangers, the harm that could be containing by such a hacker expand on the skilled of the Hacking. [7]

### 3.2 Network security Layers

Implementing advocacy in altitude is essential for enterprise network, it gives security at many layers.

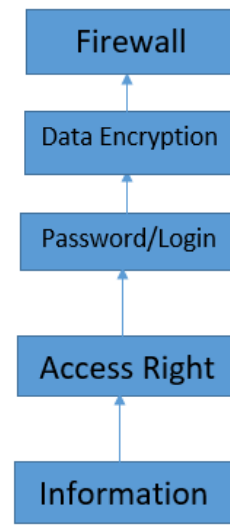


Figure 3.1: Network security layers

#### 3.2.1. Physical Layer

The physical layer is responsible to transmitting information over system correspondence media. It could also referred as most changeable and venerable layer. At the point when conduct with this sort of layer, unserious matter like unplugging the PC control rope or squandering system link could sporadically cause an incredible and untraceable destruction on an individual system, and it could reason extraordinary damage to the PC.

There are a great deal of vulnerabilities that the physical layer is standing up to, few of which include: loss of characteristic control, the mischief of equipment and data, separation of physical information joins, control harm, input logging like keystroke and other physical taking of information and equipment, and imperceptible block attempt of information. These vulnerabilities could make extraordinary damage organize security through physical layers if denial isn't done at the ideal time. By and by, there are dependably results accessible for any shakedown of harm caused to a system.

### **3.2.2 Data Link Layer**

This is where sending of information of data packets has been prepared by the physical layer. Contact of the information interface is by one way or another ineffectively as far as security. The key material at layer 2 correspondences is the switch, which is additionally utilized for correspondence at layer 3. The information interface is fit for some layer 3 attacks. The prime case of the layer 2 components is 'war driving' the strategy for circumventing looking for remote LAN (802.11) Network with default security settings. VLAN in layer 2 switches are additionally responsible to assaults or attacks.

All the OSI layer face various threat that affects them at their different stages. Featured beneath is the issue looked by layer two of the OSI level and the answer for the issues. CAM (Content-Addressable Memory) table flood, MAC (Media get to control) parodying, STP (Spanning Tree Protocol) Manipulation, ARP (Address Resolution Protocol) assault, and VLAN bouncing are the inquiry looked by information interface layers. CAM can be restricted by arranging port security on the change so as to give a MAC address particular on an individual switch port with the goal that it very well may be prepared and remembered by the port to find an invalid location on the port. Like in CAM, port security request can likewise be utilized to lead MAC-parodying.

### **3.2.3 Network Layer**

The network layer is an ordinary utilized by packets to get to their last goal over different information. As said before in the previous section above, for all intents and purposes every one of the layers have a protest to security. The least third layer of the OSI display is known to confront protest of data security issues and Denial of Service assaults. Web convention (IP) is the all-around educated convention for the system layer. There is various security issue related with the IP in the system layer. The piece of the security hazard influencing system layers is organize layer bundle sniffing, course caricaturing, And IP Address Spoofing.

### **3.2.4 Transport Layer**

The transport layer submit the two utilization of instruments, for example, TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) to deal end-to-end correspondence serving, which suits information to completely touch base at its goal. Poor treatment of questionable conditions is one the issues this layer is

confronting. Abuse of an extraordinary port for different works could likewise be a defenselessness of transport layers and in addition poor blending of vague conditions, transport convention forming contrasts, transport-layer components overburden. Firewall routine that can be utilized to confine section to designated transmission conventions and Sub-rule data ought to be strict.

### **3.2.5. Session Layer**

The session layer keeps the method for information interchanges and structures them into a shape stream. This layer likewise set, oversees, and ends sessions among advances and deals with the information exchange between introduction layer elements. Aggressors can reason damage to organization's system with this medium by boundless endeavors to speculation the secret phrase, and they can also submit utilization of cruder guidelines to debilitate doable secret key strings. The shortcoming of client confirmation instruments, capturing, and ridiculing of session recognizable proof, fizzled validation endeavors could prompt data spillages, and boundless fizzled sessions can assist aggressors with accessing certifications.

### **3.2.6 Presentation Layer**

The Presentation layer job with administration want duty from the application layer and administration ask for acquaint with the session layer. The introduction layer is known for three standards: encoding and interpreting data, scrambling and unscrambling data, compacting and decompressing data.

In spite of the fact that the Presentation layer is a standout amongst the most secured layers among the OSI show, it has its own conduct. The dangers general to this layer are phony testament assaults and man-in-the-center assaults. Care ought to be captured when taking care of sudden info since it can crash applications, security guard could be set by cryptography imperfection and remote control or data spillage could happen when utilizing outer issue input unexpectedly.

### **3.2.7 Application Layer**

The application layer is close to the end client and it enables clients to connect with the intrigue and the systems. This interface could be a practical objective for Standard security control is circumvent through the indirect accesses and application plan. In the event that security rules compel approach isn't sufficient, it results in the over the top accessor lacking access; when application security is excessively hard, it is now

and again hard for clients to access; and program rationale imperfections could some of the time cause projects to crash or ineligible conduct. [7]

Application	Application types attacks, Buffer overflows, Explode code, Malicious software i.e., Worms, Viruses, Trojans
Presentation	NetBIOS specification, Clear content extraction and convention protocol assault or attack.
Session	Session hijacking, SYN (synchronization )attack and Password attack
Transport	Port scanning, DoS attack, service enumeration and Flag manipulation
Network	IP(Internet Protocol) attack, Routing attack, ARP poisoning, MAC flooding and ICMP assaults
Data Link	Passive and active sniffing, MAC spoofing and web cracking
Physical	Hardware hacking, Lock picking, Physical access attack, wiretapping and intercepting.

Table 3.1: OSI layers Attacks

Security, it must be underlined fundamentally that the entire system ought to stay secure. System security does not just stress the security in the PCs at each finish of the correspondence rope. When sending information the correspondence channel ought not to be evincible to assault, where the likelihood of dangers is all the more entering. A conceivable hackers or attackers could objectified the correspondence channel, accomplish the information, and decode it and re-insert a wrong message. Consequently, anchoring the system is similarly as vital as anchoring the PCs and encoding the message which we need to be kept private. [1]

### 3.3 Physical Installation Attack:

Physical installation or physical layer types attacks, as the name, uncover make from some essential dangers that we can see with claim eye however probably won't be ceased. Initially, equipment risk is a general case of a physical establishment assault; this could be payable to the maturity of an exceptional framework, and as a result of that, it begins acting whimsically and hurt a few information before it all over bites the dust.

The ecological risk, as saw already, can be contained by characteristic wonders, for example, outright climate temperatures, quakes, and tempests. The electrical risk can make across the board harm a system. This way of risk is general in nations where the power supply is constantly cut out of the blue. Outline of this sort of risk is power

outage (startling boundary of the power supply), brownout (lacking supply of intensity voltage), and clamor (unconditioned power). [7]

### 3.4 Device Communication Attack

Actually fitting hackers have possessed the capacity to mold an organized assault focused at communication conventions. The OSI design has seven layers that are utilized for communication into systems administration instruments, which are with vulnerabilities that can be regularly. Essentially, the upper layers can't be anchored while the lower layers are additionally not being ensured, yet as of late there has been restricted ill will to uncertainties at the physical layer or information connect layer regardless of option in system exercises practice that develops enhancement like across the nation layer two systems what's more, national and endemic optical systems.

Presently, known dangers at lower value of the OSI stack cover ARP parodying, MITM (man-in-the-center) assaults at layer two, and physical layer assaults, for example, latent optical taps or the capture of remote system motions by the charger.

### 3.5 Typical Enterprise Network security Design

Figure 3.2 shows that a typical Enterprise Network security as an example, the implementation Architecture that designed to protect and connect numerous parts or major section of an enterprise network. This is the most general model as according to the area of the network. [2]

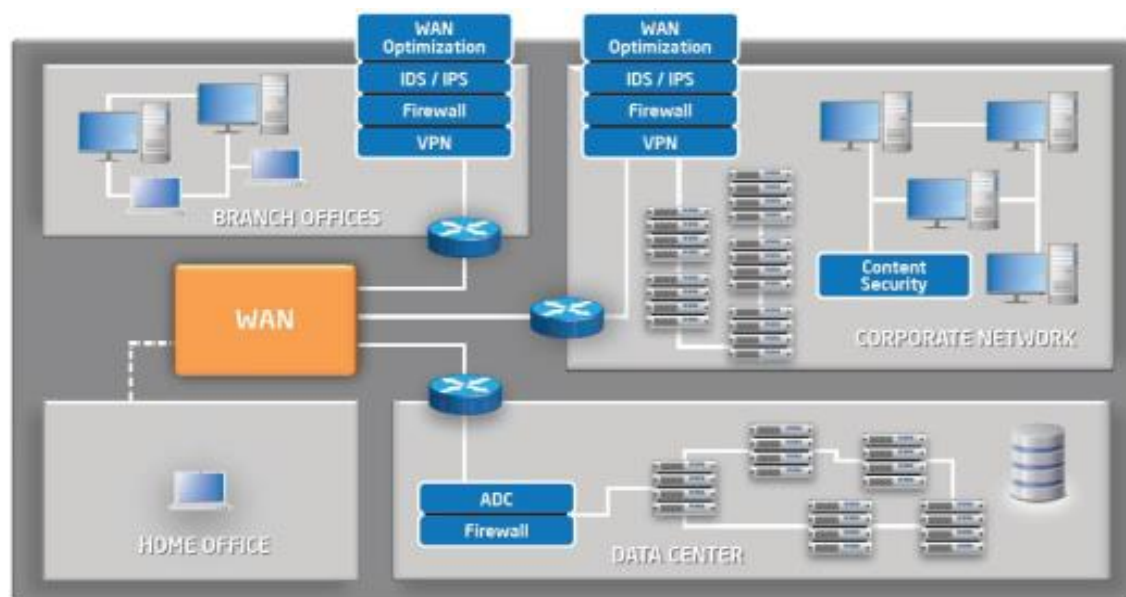


Figure 3.2: The different kinds Security steps present in the Enterprise Network



### 3.5.1 Virtual Private Networks (VPNs)

Virtual Private Networks are used to secure connection between two remote sites. They use encryption and authentication to impervious connection, VPN creates a tunnel by the public network such as the Internet to transmitted data. There are many VPN protocols that are used for VPN connection. Point to Point tunneling protocol PPTP is one of the oldest VPN protocol, it is the least secure protocol. Layer 2 Tunneling Protocol with IPSec gives better security, it accepts encryption of header and payload. L2TP/IPSec is protected than PPTP. Open VPN is another VPN protocol, it is the most used protocol nowadays. In our research thesis, we bring in a security-enhanced pattern of an enterprise network that acts network security integrally. [1]

### 3.5.2 Firewall

A firewall can be either hardware-based or host-based. A hardware-based firewall as a rule implies specific system boxes, for example, routers or switches, containing altered hardware and software based configuration. This sort of firewall is frequently costly, confused and hard to arrange. Rather than a hardware-based firewall, a host-based firewall is less demanding to use for people or little associations. A host-based firewall can be comprehended as a bit of programming running on a person's PC, journal or host. It is intended to permit or confine information exchanged on a system based on a lot of guidelines. A firewall is utilized to shield a system from interruptions and simultaneously enable genuine information to go through. Ordinarily, a firewall ought to have something like two system exchange, one for private system and another for open system activities, for example, the Internet.



Figure 3.3: Firewall

### **3.5.3 IDS/IPS**

IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) both are applied for the ensuring security level of in a big networks as well as control traffic and inspecting and considering govern packets for suspicious and also for malicious data. In the way of Discovery in existing or given identified systems is mainly performed by the signatures and whereas the findings detected and identified in that systems. The major variation between one system and the other is the action they take when an attack is discovered in its primary steps (especially in network scanning and port scanning).

- The Intrusion Detection System (IDS) provides as the way of network with a level of preventive security against any suspicious activity. The IDS earn this motive through early warnings aimed at systems managers. However, unlike IPS, it is not planned to block attacks.
- An Intrusion Prevention System (IPS) is a device that controls access to IT networks in order to protect some major systems from attack and abuse. It is planned to inspect attack data and take a similar and immediate action, blocking it as it is an incentive and before it succeeds, making a series of rules in the corporate firewall, for example. [9]

### **3.5.4 WAN Optimization**

WAN optimization, also known as WAN acceleration, this class belongs of some valuable technologies and techniques that is used to maximize the skill of data flow crosswise a wide area network. As we already saw that in an enterprise WAN, the goal of optimization is to increase the speed of access to critical applications and information. [10] [11]

Advantages of WAN optimization-

#### **3.5.4.a Data Protection:**

Data protection contains or referred Secure all traffic across Hybrid WANs among Steel Heads for Private (MPLS) and Internet Links with standards-based encryption for added security and regulatory assent.

#### **3.5.4.b Problem Resolution**

Resolve problems faster with high IT visibility into application, network and end-user knowledge.

CHAPTER 4  
PROBLEM STATEMENT OF AN ENTERPRISE NETWORK

## **PROBLEM STATEMENT OF AN ENTERPRISE NETWORK**

Most of the organization found out that their existing security system controls are reducing their effectiveness and preventing them from getting something done. An organization needs to share some information with new colleagues, client or the overall population. The security issue is a factor for business because it causes an impact on business so security program needs to be effective, it must show an incentive to the business while evading the customary traps related with the impression of security currently turned into a deterrent and bother to viable business tasks. So the risk depends on the security system and security policy that the administrator applied on the network. Sometimes good security of an organization creates a good business opportunity because the customer, business partners want to be sure that their data is secure as new risks are introduced daily so administrator needs to be aware of everything and should apply a proper firewall policy to prevent those attacks & risks. So the company needs to balance the security issue and business information while sharing company information with employees to be productive and share information easily.[12]

### **4.1 Problem IN Existing system**

- ❖ IP spoofing.
- ❖ Insider intrusion.
- ❖ Direct internet traffic.
- ❖ Denial of service (DDOS).
- ❖ No protection against masquerades.
- ❖ Firewall trust on trusted network (LAN & WAN)
- ❖ Firewall doesn't scan virus on network traffic as processing speed fact.

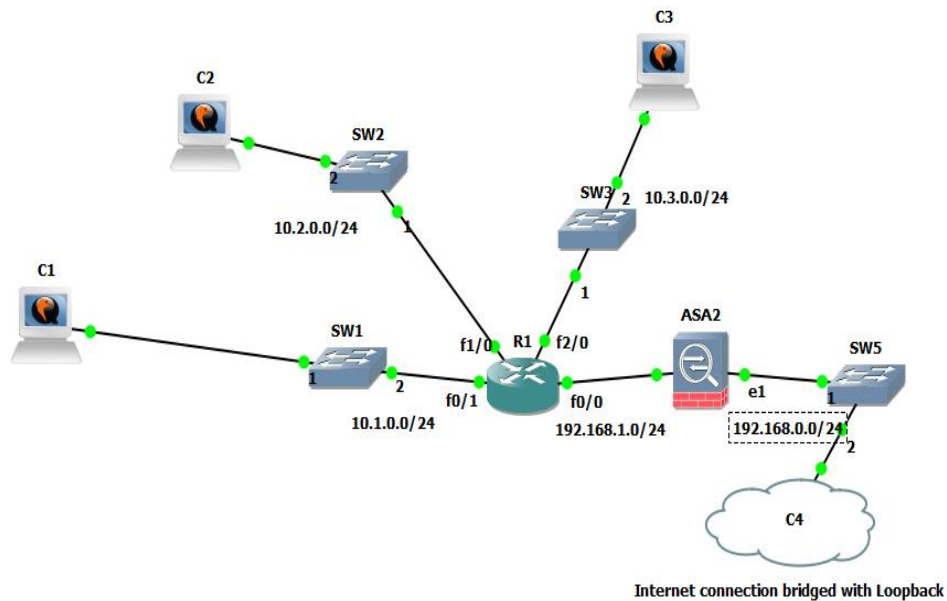


Figure 4.1: Existing Network Model of an Enterprise Network

#### 4.1.1 IP Spoofing

To procure unapproved access to PCs IP spoofing is kind of method that attacker use. In this process, the insider sends ill-conceived messages to a PC with IP address that demonstrates the message is originating from a trusted host. Before starting IP spoofing attack, hackers uses different type of method to find a trusted host with its IP address then attacker modifies his packet header with the packet are coming from trusted host. So as to create traffic and make it originating from a trusted host attacker engage the unsuspecting hosts and then flood the network.

#### 4.1.2 Insider Intrusion

Insider intrusion is kind of unusual type of attack it is not like external threat ,A person who is authorized system access could be an insider intrusion attacker, So there may be less security against insider intrusion on most of the organization because most of the company focus on their external attacks, Insider threat is kind of insider attack.

#### 4.1.3 Denial of service (DDoS)

More than one computer attack a target from different location such as a server, website or other network assets on a distributed denial-of-service (DDoS) attack. Due to this attack a full network flooded by an incoming message, a connection request or

malformed packets to the target for that reason the target system forces to slow down or crash and even shut down.

#### **4.1.4 No protection against masquerades**

This attack run by using a fake identity which is same as a network identity to gain unauthorized access to PC data through authentic access reorganization. To avoid a masquerade attack at first need to completely ensure all kind of authorization process is fully protected otherwise it will be vulnerable to attackers. By utilizing stolen passwords and logins Masquerade attacks can be executed, it could be utilizing also by finding a bug in programs, or by finding a trace around the verification procedure. The assault can be actuated either by somebody inside the association or by an outsider if the organization is connected to an open network. The amount of access masquerades attackers get depends on the level of authorization manage to attain.

#### **4.1.5 Firewall trust on trusted network (LAN & WAN)**

When the LAN is associated with another LAN or the Internet and turns into a WAN, the majority of that changes. The organization does not recognize what physical securities have been made to whatever remains of the WAN, just its little bit. On account of an Internet association, they have no clue who may endeavor to get to their LAN. The whole risk display changes. Not unreasonably any of the dangers from the LAN-just condition have left, yet a lot more have been included. One can think about the danger profile for a LAN similar to a subset of the risk profile for a WAN.

Security measures are appropriate or not depend on the threat profile that helps us to understand network management for a self-connected LAN network, Here no need to have network management protocol encryption or special authentication for those protocols, Network administrator does not want his network management protocols to traverse without the special authentication of internet protocols, So for any system first step is to identify the threat and then apply threat prevention policy to ensure security protection.

## 4.2 Proposed Model for an Enterprise Network

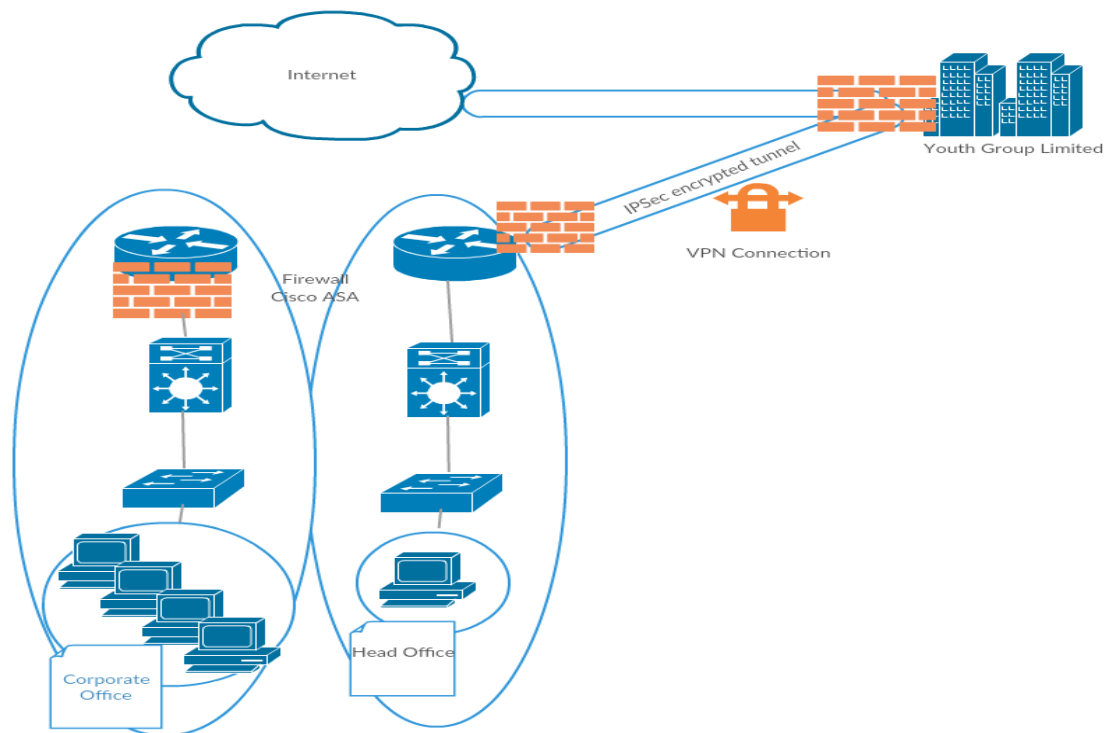


Figure 4.2: Proposed model

Proposed mode may overcome the above all existing problem of an enterprise network. Here are those probable improved part of the model given below:

- ❖ Strong Authentication.
- ❖ High Data Security.
- ❖ Multilevel Protection.
- ❖ Network Traffic Encryption.
- ❖ No Insider Intrusion.
- ❖ Strong Masquerades.
- ❖ IP sec used.
- ❖ Port forwarding.
- ❖ Internet traffic filtering.
- ❖ Different web access policy for users.

#### **4.2.1 Strong Authentication**

Minimum two different authentication factor of different types to improve the safety of identity verification is the true fact of strong authentication, Password will not be plain text and a level of security will be ensured for password and system security improvement policy will be added. A weak password is easily venerable to the attackers by using snooping, borrowing and dictionary attacks so strong authentication is required to minimize the risk of involving these high-value systems. Installation of two authentication factor instead of one authentication will provide an advanced level of authentication assurance.

#### **4.2.2 High Data Security**

Information security is the way toward protecting information from unauthorized access and information debasement for an incredible duration cycle. Information security incorporates some procedure like encryption, tokenization, and key administration, The organization around the globe are investing on heavy it technology (IT) cyber defense capabilities to protect their critical assets, An enterprise needs to protect its various type of data from unwanted attackers for that high data security assurance is the must.

High data security includes below fields...

- ❖ Cloud access security
- ❖ Data encryption
- ❖ Hardware security module
- ❖ Key management
- ❖ Enterprise data protection
- ❖ Payment security
- ❖ Mobile app security
- ❖ Web browser security
- ❖ Email security

#### **4.2.3 Multilevel Protection**

Multilevel Secure System is a class of frameworks containing data with various sensitivities that at the same time allows access by clients with various security clearances. The idea behind MLS is that a system must be able to enforce the mandatory security policies over classified data, accessed simultaneously by clients



with various clearances and need-to-know, and to preserve the fulfillment of the applied security models. An MLS system is typically dependent on a various leveled get to control display that is established on a standard tiling called grid. The tackle is known as Mandatory Access Control (MAC): the user cannot disable or bypass it. On the inverse, there is the Discretionary Access Control (DAC) that anticipate to filing owners the obligation to enforce the access control policies. In the final case, the owner of the file can unwillingly or intentionally violate the policies by simply tempering the access permissions.

#### **4.2.4 Network Traffic Encryption**

Network encryption is essentially executed on the system layer of the OSI model. Network encryption actualizes at least one encryption calculations, procedures, and standards to encrypt the information/message/packet sent over the system. The encryption administrations are for the most part given by encryption programming or through an incorporated encryption calculation on system gadgets as well as in programming.

On an IP-based system, arrange encryption is actualized through Internet Protocol Security (IPSec) based encryption procedures and benchmarks. Each message sent is in an encoded shape and is unscrambled and changed over again into the plain content/unique frame at the beneficiary's end utilizing encryption/decoding keys.

#### **4.2.5 IPSec**

There are two processes for security on IP packets, The Encapsulating Security Payload (ESP) protocol, which characterized a technique for scrambling information in IP packets, and for digitally signing IP packets a method defined by the Authentication Header (AH) protocol. The cryptographic keys used by hosts for IPsec is the Internet Key Exchange (IKE) protocol which is used to manage IPsec can be used to protect network data, for example, by setting up circuits utilizing IPsec tunneling, in which all information being sent between two endpoints is scrambled, similarly as with a Virtual Private Network (VPN) association; for encoding application layer information; and for giving security to routers sending encrypted information over the public internet. IPsec can also be utilized to give authentication without encryption, for instance, to verify that information originates from a known sender.

Internet traffic can be set up circuits utilizing IPsec Tunneling, in which all information being sent between two endpoints is encrypted, similarly as with a Virtual Private Network (VPN) association; for encoding application layer Information; and for giving security to switches & routers sending directing information over the general public internet. IPsec can likewise be utilized to give verification without encryption, for instance, to verify that information begins from a known sender. Web traffic can be anchored from host to have without the utilization of IPsec, for instance by encryption at the application (Layer 7 of the OSI show) with HTTP Secure (HTTPS) or at the vehicle (Layer 4 of the OSI demonstrate) with the Transport Layer Security (TLS) convention.

Secured from host to have without the utilization of IPsec, for instance by encryption at the application (Layer 7 of the OSI display) with HTTP Secure (HTTPS) or at the vehicle (Layer 4 of the OSI show) with the Transport Layer Security (TLS) convention. However, when traffic uses encryption or authentication at these higher layers, threat actors may still be able to intercept protocol information that may expose data that should be encrypted.

#### **4.2.6 Port Forwarding**

Port forwarding, also called tunneling, is basically the way toward catching traffic headed for a specific IP/port blend and diverting it to an alternate IP and additionally port. This redirection is cultivated by an application running on the destination host, or it is performed by moderate equipment, similar to a switch, intermediary server or firewall. Typically, a routing device will look at the header of a packet and simply send it to the proper interface to reach the destination it finds in the header. In port forwarding, the intercepting application or device reads the packet header, takes note of the destination, however, revises the header data and sends it to another host destination, not the same as the one asked. That has a destination is an alternate IP utilizing a similar port, an alternate port on a similar IP, or a totally extraordinary blend of the two.[13]

IPs and ports to the assignment inside. This is exceptionally valuable for individual system clients, who may wish to run an FTP server, a Web server and a gaming server on one system. Clients with this kind of necessity set up a single public IP address on the router to make a proper translation request on the proper server of the internet. This process has the benefit of hiding away precisely what administrations are

running on the system, utilizing the main IP deliver to complete various assignments, and dropping all traffic at the firewall unrelated to the services provided [13].

#### **4.2.7 Internet traffic filtering**

Internet Traffic Filtering (ITF), is a mechanism for blocking distributed denial of service (DDoS). These attacks are an intense contemporary issue, with a couple of practical solutions available today. We applied policy on the firewall to prevent these problems.[14]

#### **4.2.8 Different web access policy for users**

The emphasis of NAC is the entrance control – who or what has approved authorization to get to the system. This incorporates the two clients and gadgets. The NAC organize blocks the association demands, which are then confirmed against an assigned personality and access the board framework. Access is either acknowledged or denied dependent on a pre-decided arrangement of parameters and strategies that are customized into the framework. NAC requires participation among conventions and diverse innovations that go from IT system to security so as to work successfully.[15]

CHAPTER 5  
IMPLEMENTATION AND EVALUATION

## **Implementation and Evaluation**

This chapter mainly focused on our main things that we want to implement and enhance our security model of our proposed system of an enterprise network. The motive of this security of an enterprise network to protect its valuable data, file, document and many other things from attackers, hackers and others dangerous platform. In order to prevent those attacks and enhance our security, we need proper authentication and authorization. In section 5.1 we will see that what kind of tools are needed for this Process to implement in enterprise network and proper evaluation. In Section 5.2 we will see that the process of policy apply like NAT, ACL , WAN and LAN zone , trust and Untrusted network determine and various thing . In section 5.3 we will see that port forwarding in LAN side to secure our potential websites, server, different devices which is accessible by internet with a major concern of security. In Section 5.4 we will see that how IPsec VPN policy is applied for higher security purpose and better authentication from vulnerability and packet spoofing is resolved from active and passive attacks. And at the end of this sector we will see that Bandwidth utilization of this proposed system that we want to implement of an enterprise network.

### **5.1 Devices and appliances**

To enhance our proposed model we draw a network architecture of our desire system and make a topology in Graphical Network Simulator-3 (In Short GNS3). In this part, we took three cisco router and two Fortinet firewall and some non-manageable switch connected with Internet cloud separately. In the existing system, the ASA 8.42 firewall is used which is costly and expensive and also have some limitation. There are different types and better-secured firewall in our Internetworking world to secure the world of the internet now in this era. Some of these firewall like Cisco ASA, Fortinet, Fortinet-Hyper version FortiGate firewall, Sophos firewall, Software firewall (Like ACL), Barracuda spam firewall etc. are available.

We will implement a FortiGate firewall in this system to enhance our security. This firewall has excellent features with flexibility and comfortability both graphically and CLI mode. Fortinet with the advance version of FortiGate has various update version that's are user-friendly and highly secured to protect our LAN and WAN portion on the Internet. Free Meter tools used for Bandwidth monitoring and bandwidth

utilization of our existing system as well as how much improved in our proposed system to obtain a better result and help to find out an effective result and also inefficiency measuring. This tools installed in host pc that means any change in bandwidth is given us the result of bandwidth utilization. This free meter tool is designed for Windows operating system which is almost reliable for Bandwidth Monitoring and also for the process of evaluation.

WinMTR is one of the free tools to lookup traceroute of a Networking device connected with the Internet. Having a connection with proper establishment with an actual route from source to destination can easily give us traceroute hop to hop and also ping statistics of a network. This is also called Network diagnostics tools that are truly named after Matt's traceroute. A Network connection with the proper route in a topology or a diagram facing any network difficulties or slow speed can be determined by the WinMTR.

Fortinet-FortiGate hyper version is a next Generation firewall with advanced features and technology that is used for higher security in LAN and WAN side as well as secure our network connection in the world of internet. In my opinion for an enterprise network Fortinet firewall is the best solution to fulfill or requirement and meet up the challenge of privacy and protection. The firewall leads the maximum efficiency in both platforms (Virtualized and Hardware). And the FortiGate Next Generation hyper Firewall that utilizes purpose-built security processors and the most harmful threat intelligence security services from FortiGuard labs to deliver top-rated protection and high performance including encrypted traffic. FortiGate reduces complexity with automated visibility into applications, users and network and provides security ratings to adopt security best practices.[1]

The devices and tools are used in this topology is given below:

Device Name	Specification	Installed Tools
Host PC – PC1 PC2 PC3	CPU: Core i4, 1.5 GHz	SecureCRT 8.5.2, WinMTR, FreeMeter
Cisco Switch	Layer 2 device ,Non Manageable	GNS3
Router c7200p	Layer3 device, Fast Ethernet port, Gigabit port , Maximum Speed accuracy	Cisco c7200 iOS, Wireshark
ASA 8.42 firewalls	Identity Firewall, Identity NAT configurable proxy ARP and route lookup	Cisco ASA 8.42 ios , ASDM bin
Firewall	Fortinet -FortiGate Hyper Versions	FortiGate VM , FortiGate-3140B
Metasploit Framework	Penetrating tools	Windows 10 Operating System

Table 5.1: List of Tools and devices for Implementation and application

Network Design: The network or topology of our proposed system of an enterprise network is given below compared to an existing System we already showed it previously.

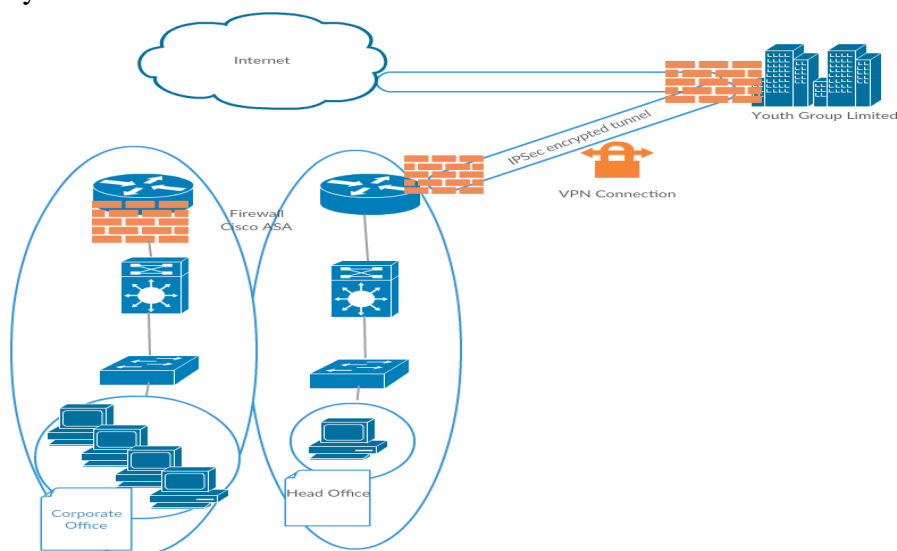


Figure 5.1: Propose Model for An enterprise network

In this topology it's a scenario of an enterprise network where Corporate office and branch office connected to head office in same network .In this topology the internet cloud connected with Fortinet firewall for concern of security, privacy and authentication .Then this Head office Firewall connected with another Fortinet firewall with encryption and using Internet protocol Security (IPSec) VPN for higher security purpose along with the synchronization with routers ,switch , L3 switch consecutively with end device (host PC). This is common scenario of our proposed network to enhance security of an enterprise network.

## 5.2: Implementation of firewall With the Integration of Different Policy:

This Section describes the different policy applied in Fortinet firewall and various steps taken to remove the different attack as those attack mentioned before and how those attacks mitigate in FortiGate firewall. As in this Network topology where the whole network is scanning by the Wireshark software find the attacks before the action is needed from the firewall. For Implementing security both the results from the network with its scanning process are compared to show whether the reconnaissance. In Figure 5.2. Shows the FortiGate-3140B Firewall Graphical Mode of IPS page with an observation of Aurora attack is detected and need to prevent it.Aurora attack is highly harmful to the entire system. It target s on the server host that take place in the Windows operating system as well as various random places that are essential for protecting data.

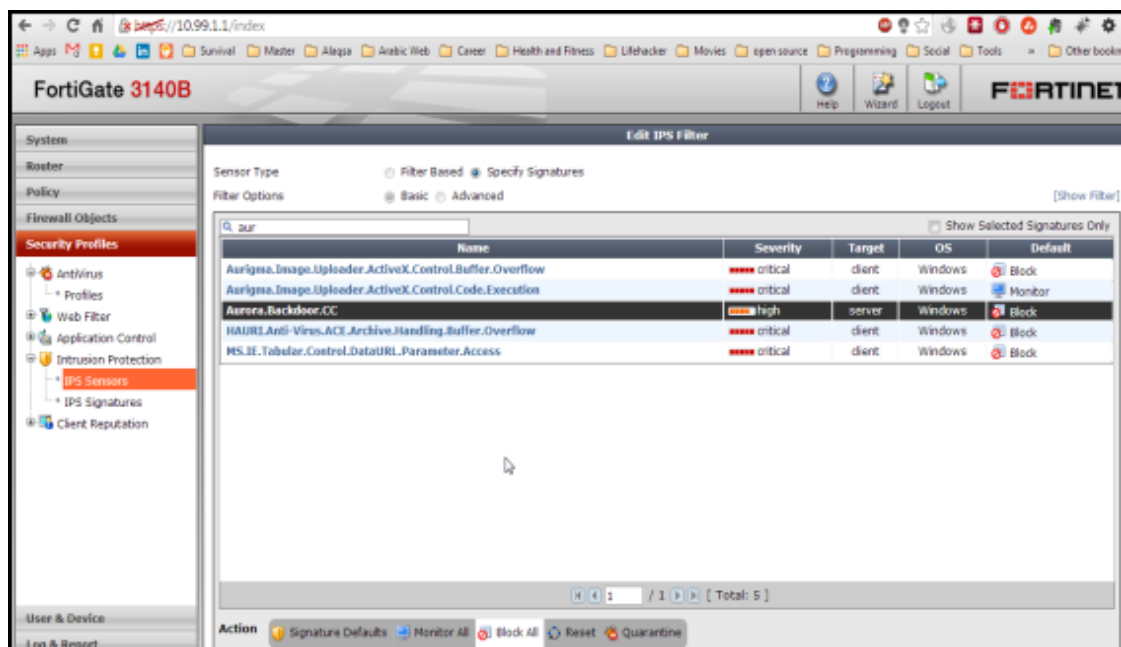


Figure 5.2: Aurora Attack take place IPS Page FortiGate-3140B



For Removing Attack and secure our data we need to protect HTTP, HTTPS, Telnet, SSH, SNMP port in firewall as well as in the router. so It's essential to configure and monitoring the firewall carefully .Setting Up the FortiGate Firewall and configured it properly .Figure (5.3) and Figure (5.4) shows that the IOs file configures in the vmware and established a connection Host PC and Virtual PC connected and setting IP and port In the for FortiGate Firewall in CLI Mode . When all the process of Configure IP and port successfully configured then then we can access the graphical Mode of FortiGate Firewall. The Assigned Ip in the port of Firewall having a Smooth Ping Statistics from source to Destination.

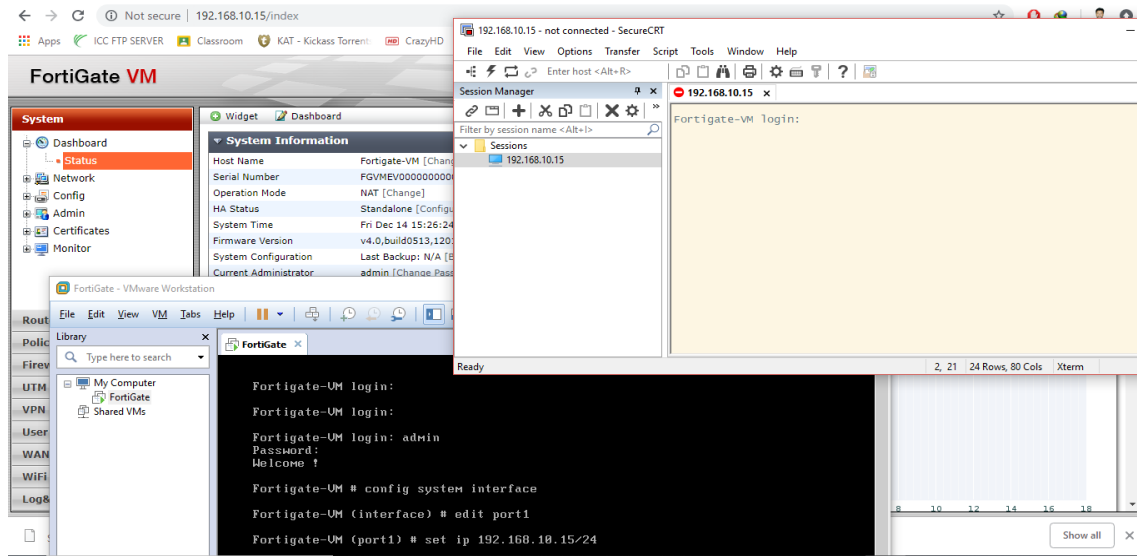


Figure 5.3: Configuration FortiGate VM with CLI Mode

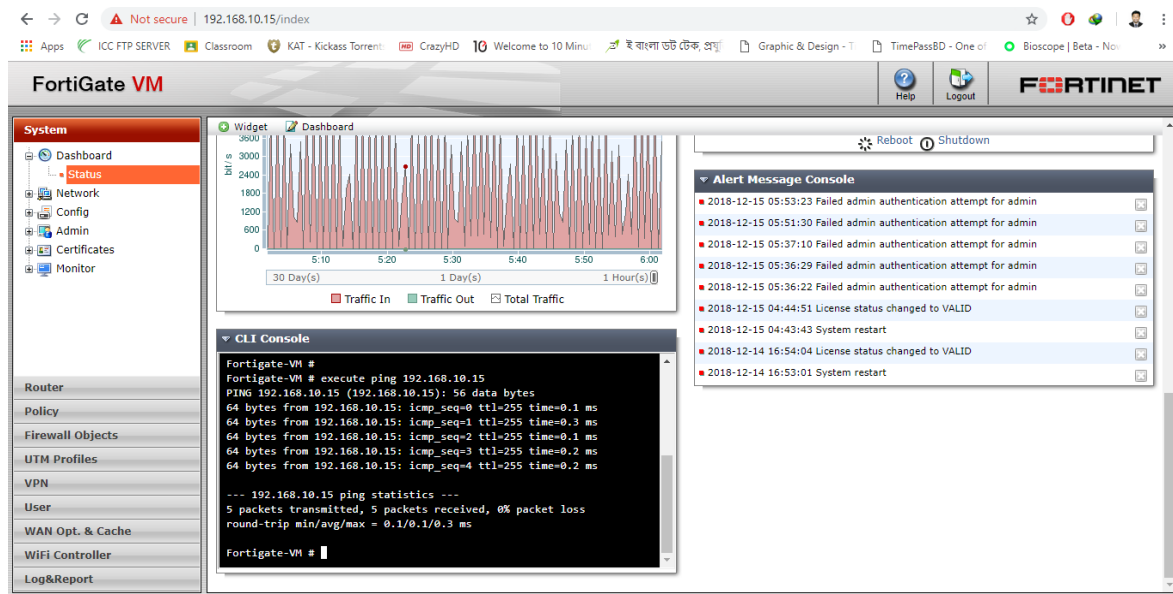


Figure 5.4: Ping Statistics of FortiGate VM with Host PC

### 5.3 Implementing Port Forwarding and Policy against Direct Internet Traffic:

Port forwarding on router or firewall or any kind Device which control or monitor traffic on the internet which allows a port address enter to it. Port forwarding plays an important role to secure vulnerable port of potential devices form attackers and hackers to keep safe our important data. With port forwarding, the internal port of a router or firewall along with an IP address can be changed where port number forwarded to unknown port for Incoming. This is a tricky way to secure and put privacy on the firewall to protect our Data.

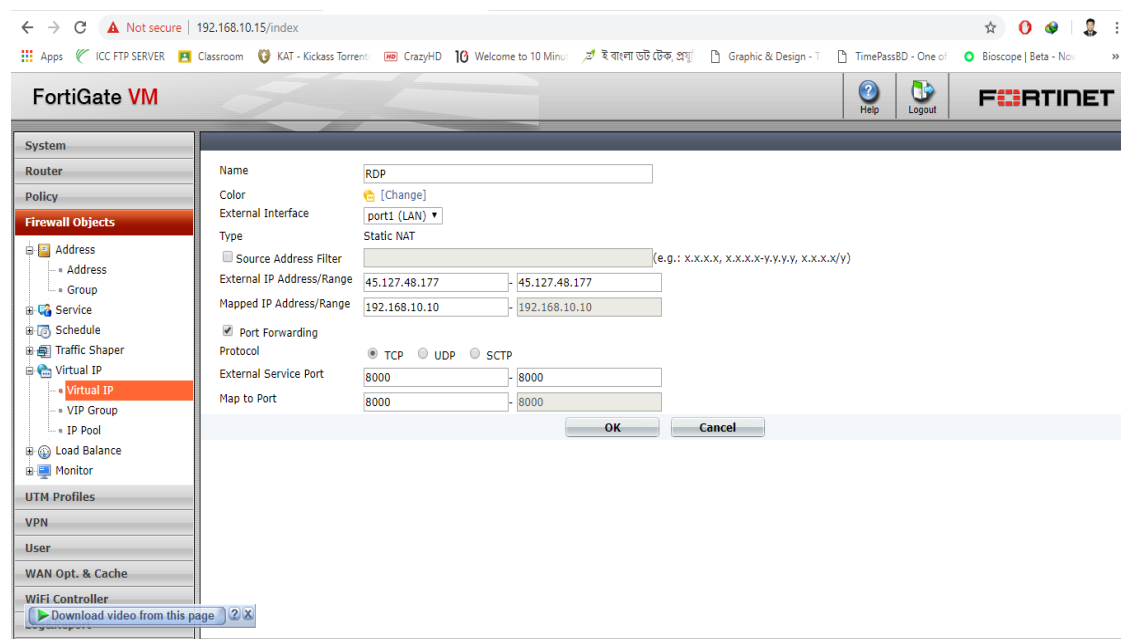


Figure 5.5: Port Forwarding in FortiGate Firewall

In This firewall, we forwarded TCP port 21 to 8000 with the Private IP mapping with public IP as it given form Internet Service provider. Port Forwarding or port mapping is part of Network Address Translation (NAT) where it is applicable. Direct Internet Traffic: Direct Internet traffic that a hacker sends a malicious virus and different kind of direct attack through third party software like uTorrent, Bit torrent and many other open source software in our window operating system with the permission of access firewall without unknowing of mind.

This an Important problem and a security concern nowadays. It can be removed by our awareness when clicking any harmful link or installing any crack open source software in our windows operating system. So we create rules and policy like Objects (IP/Subnet, FQDN)create in FortiGate Firewall and Introduced them in particular declaration with these specific objects. These objects are blocked from firewall where



And the Traffic for direct internet monitoring shows in figure (5.8), in that monitoring gives us a concept or knowledge about direct traffic filtering in incoming and outgoing. We can understand from this figure that how much problem occurs in direct internet traffic.

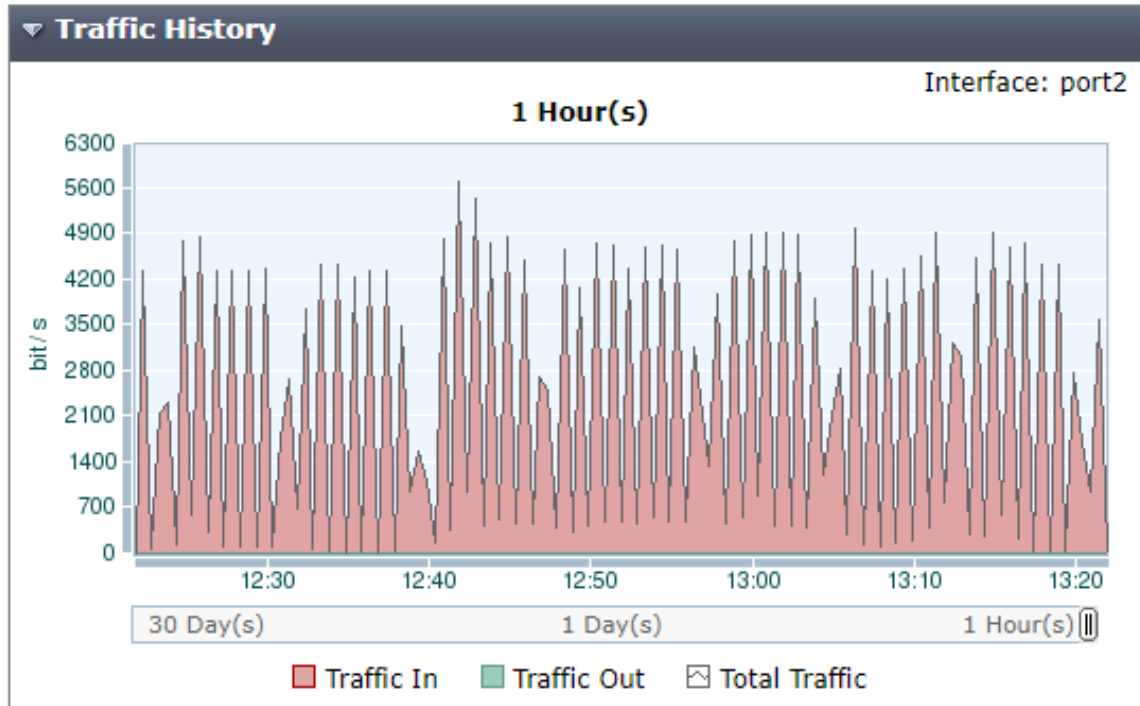


Figure 5.8: Traffic History of Direct Internet traffic ingoing and outgoing

#### 5.4 Implementation of Internet protocol security (IPsec) VPN in Proposed Model:

The IPsec is used for Better security, IETF standard protocol. It supports secure Internet Protocol (IP) layer communication. This method widely used to perform VPNs either as a full-fledged security gateway sitting between the corporate network and the router connected to the Internet or as part of the router itself, IPsec and an associated suite of protocols offer complete cryptographic security. IPsec provides the essential infrastructure to spread of an enterprise's private network as well as the Internet to spread out to various clients and business partners as well as to make that is especially called a "virtual private network (VPN)".

It maintains the encryption process in sending data one place to another. The IP layer is being secured when data is sending with an encryption process. A cryptographic key and also pre-shared keys use during the session. In our proposed model we

applied IPsec Vpn between two FortiGate firewalls which have a secure process in a big enterprise network in order to prevent Intrusion and different kind of threats. For a session with the end to end security, IPsec VPN provides the best TCP/IP layer security along with higher levels of authentication. In WAN port LAN port where there is a route between source and destination, a pre-shared key is used for remote connection in FortiGate firewall to another destination firewall with a virtual private connection is established. A tunnel is established Between head office to corporate office with IPsec Vpn for the purpose of secure data internet passing and creates strong zone apart from the outside world as well as Internal network have several conditions of firewall policy when file sharing or data.

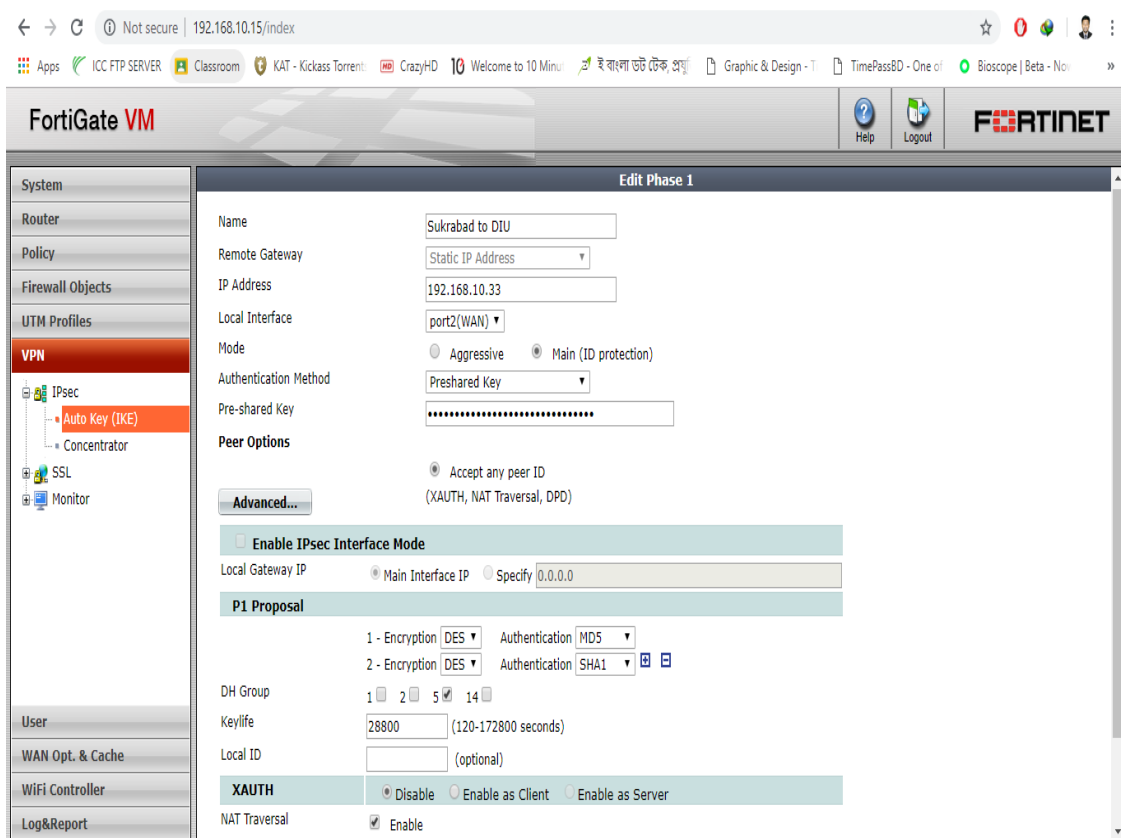


Figure 5.9: VPN Configuration in local Interface for remote host

Another IPsec VPN configures in the remote destination in the same way along with pre-Share keys encryption, remote destination address, and Port(LAN) Selection. Figure (5.10 & 5.11) shows that the configuration of IPsec VPN for destination Host. The best path choose to give encryption make a session with local Host. And the firewall Policy applied in the FortiGate Firewall.

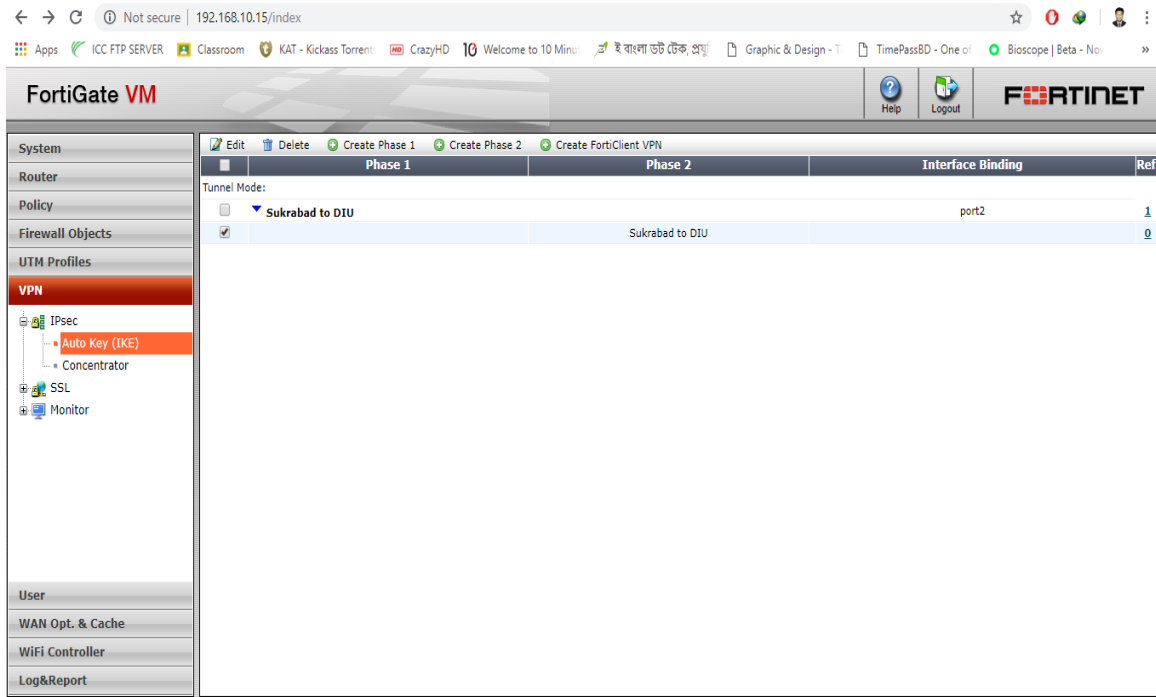


Figure 5.10: IPsec VPN Configuration in Both interface of LAN and WAN port

### Interface of LAN and WAN port

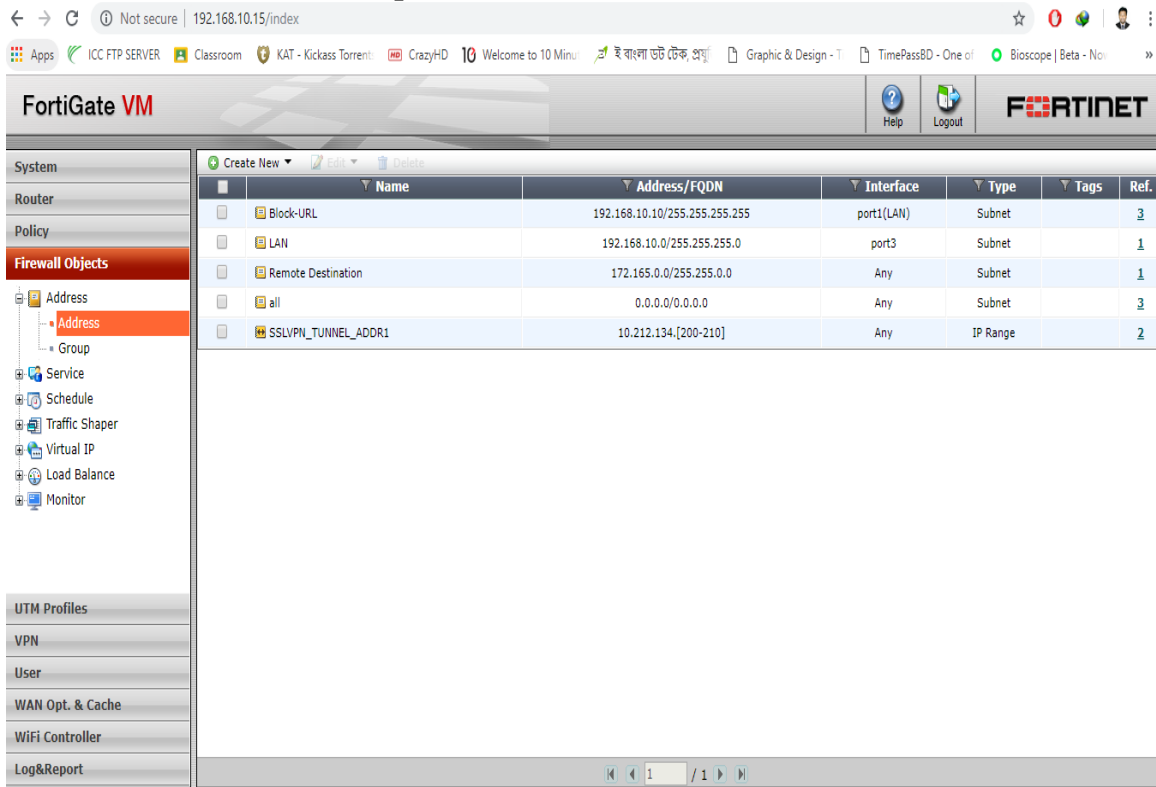


Figure 5.11: Firewall policy for IPsec VPN

**5.5 Results:** In this paragraph the evaluation of the outcome by applying the various policy, rules and various configuration has been done in Fortinet\_FortiGate Firewall. The following figures show the result of port forwarding, Protection against DoS Attack, Direct Internet traffic, Port Scanning, and IPsec VPN. These evaluations for the proposed System of an Enterprise Network. Using the Metasploit tool for the penetrating attack in the FortiGate firewall. And this penetrating attack are done with various purposes like port scanning and Aurora attack for evaluation of log report in FortiGate firewall. Figure 5.12 shows that that penetrating attack by the Metasploit tool in order to detect Aurora attack, port scanning in the in the FortiGate firewall. In our findings in the exploit of a vulnerability in firewall using Internet Explorer with local Host.

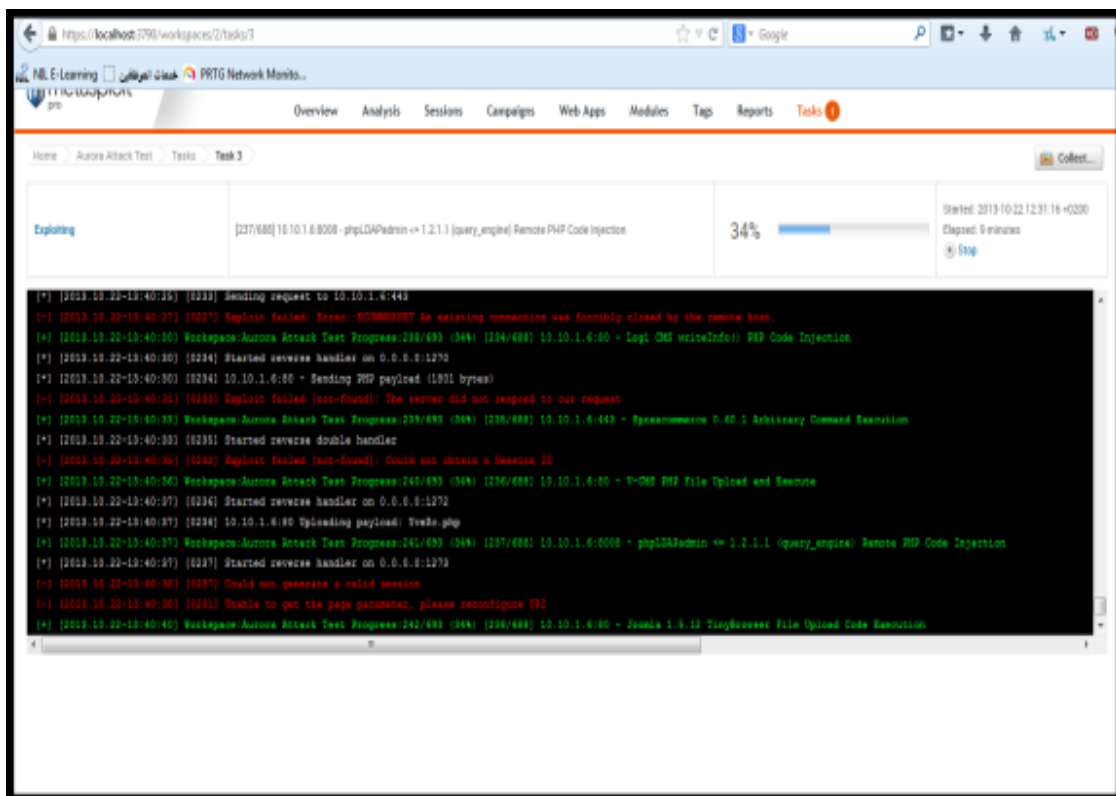


Figure 5.12: Launching Aurora in Metasploit Tools with Port Forwarding

Some Object of Aurora attack with ip address and port in the fortigate firewall. The vulnerability scan and log report Generate from fortigate firewall is given below in figure 5.13 and 5.14

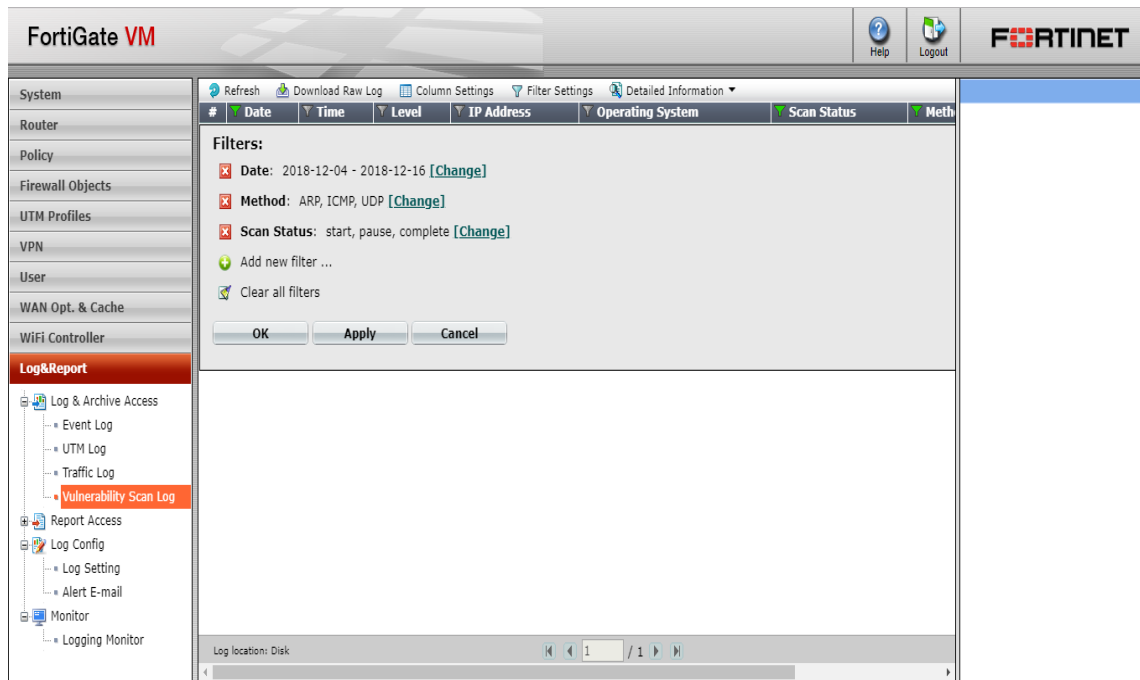


Figure 5.13: Vulnerability Scan log in FortiGate Firewall

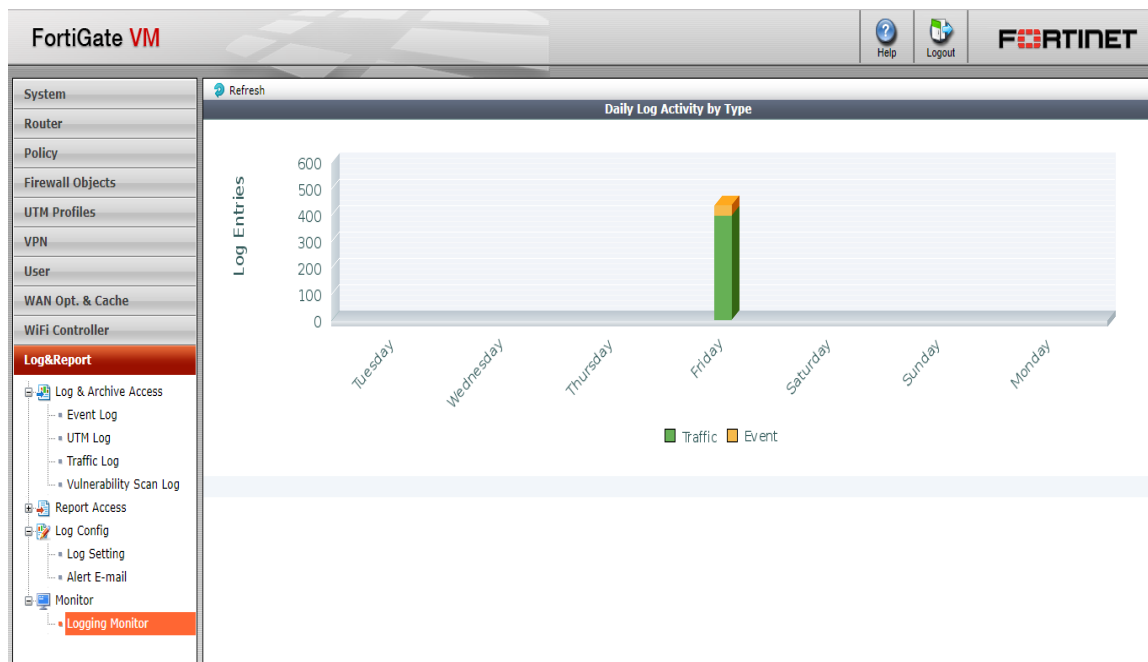


Figure 5.14: Log Monitoring In the firebase of FortiGate

## 5.6 Performance Analysis and Evaluation:

We have used free meter tools to Monitoring and utilization of Bandwidth in Proposed system of an enterprise Network compared to an existing system. One more thing to say Fortinet firewall is comparatively cost effective and Reliable than ASA



(Adaptive Security Appliances). On the other hand, ASA firewall is costly though reliable when we think to design a network topology for an enterprise network. Firstly, we think how much cost reducing when buying the network equipment. An effective network topology is not only helpful and necessary for an enterprise network but also efficient and useful for a company.

When we applied different policies and rules in the firewall to protect our data from attackers or hackers, then bandwidth is also a concern. We use free meter tools for measuring and monitoring bandwidth utilization when all the processes are running in the firewall. Figure 5.15 shows bandwidth utilization before applying the proposed model, and Figure 5.16 shows the bandwidth after using the firewall as the procedure already mentioned before in this paper.

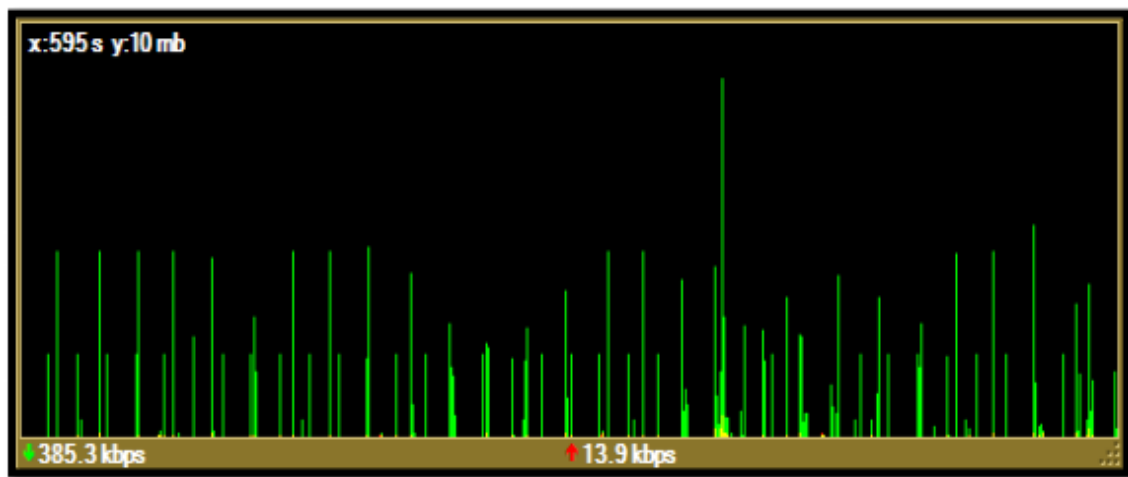


Figure 5.15: Utilization of Bandwidth before applying the Proposed Model

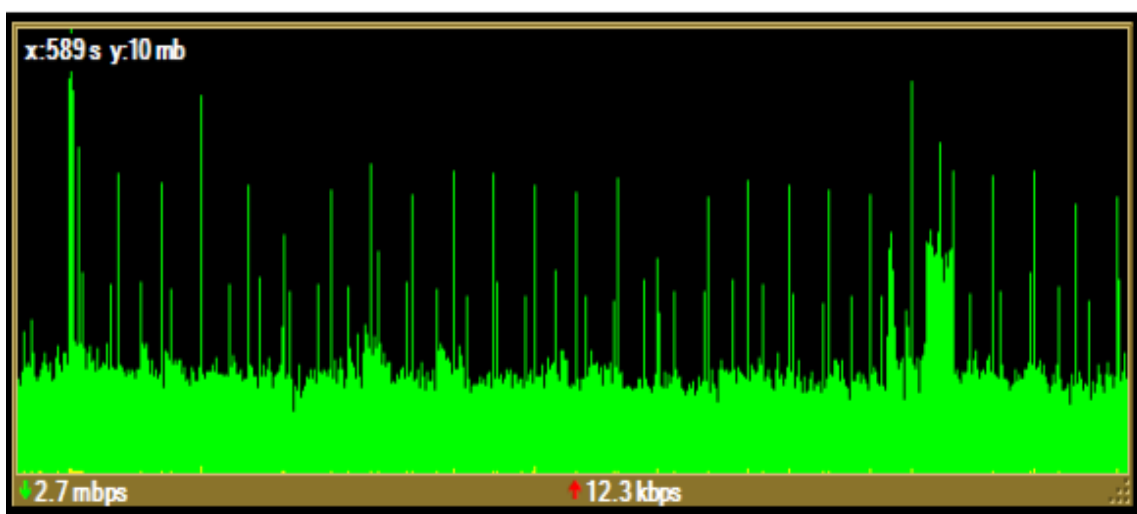


Figure 5.16: Utilization of Bandwidth after using Firewall

So comparatively Bandwidth utilization in our proposed monitoring System is better than existing system considering maximum usages of maximum traffic. And we get CPU Usages is moderate than existing System. If we differentiate attacks between Proposed system and the existing system in a chart of graphical view that it will be easier to Understanding and we will find out Anomaly of these systems. From figure 5.17.

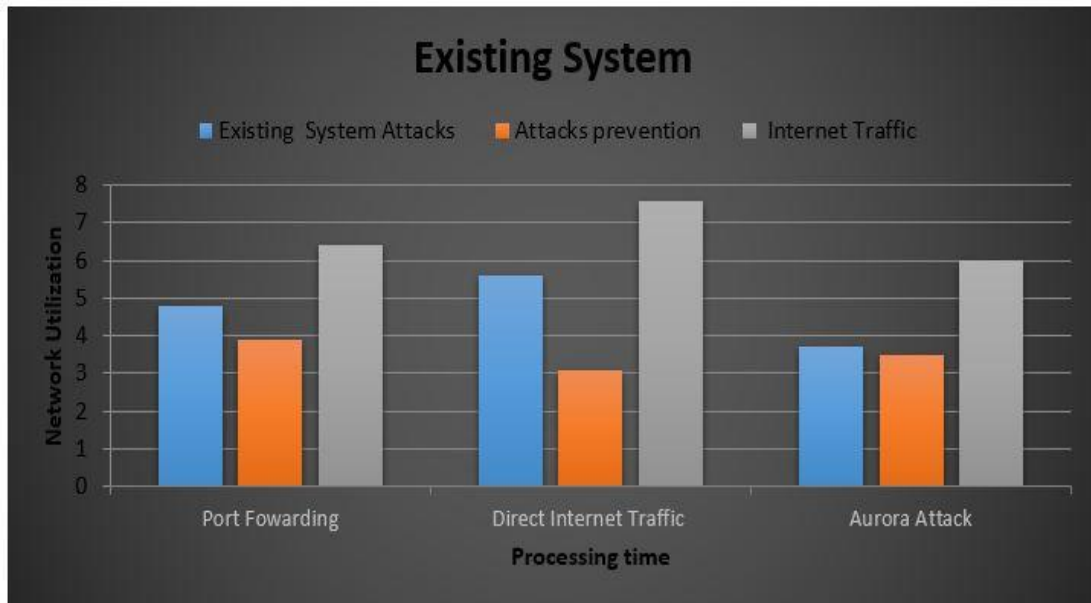


Figure 5.17: Existing System

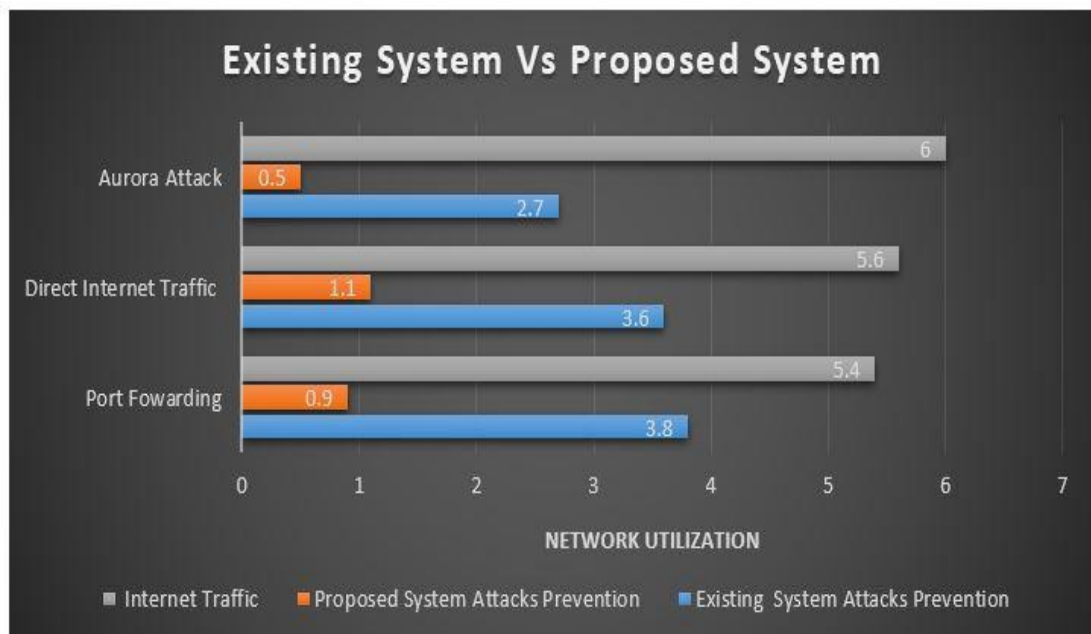


Figure 5.18: Comparison between Existing and Proposed System.

CHAPTER 6  
CONCLUSION

## Conclusion

In this project, we developed a network enhanced model for an enterprise network. Basically, an enterprise network includes a different device, network, equipment, and protocol. Different device connected in a different layer. In layer two different devices like switches, printers are connected to the network. And layer three core switches like routers are connected to the network. These core switches are used to connect different branches in the different network. Basically, an enterprise network attacked by many threats like external and internal threats. Also, attacks came from different layers. To prevent this attack enterprise network uses different devices like VPN, firewall.

Firewall is used for filtering the traffic which comes from the internal or external network. A firewall can be either hardware based or host based. Different firewall used in a different layer. Based on the network criteria firewall is implemented in the network. Virtual Private Network (VPN) is used to connect to different networks which are located in the different area for securing data. VPN creates a tunnel to secure private network from the public network. Basically, an enterprise network creates by interconnects different LAN and WAN. Also, there are different requirements of enterprise network such as availability, security, redundancy, reliability, scalability. These requirements make enterprise network reliable.

Security threats become a big challenge to create an enterprise network. The proposed network model in our thesis also an enterprise network. This enterprise network is affected by different threats like IP spoofing, Phishing attack, DoS attack, spyware attack etc. The proposed model gives a better solution to prevent the attack. As an enterprise network security issue is critical we deployed firewall and VPN to protect the network. In our thesis, we keep studying to our model to prevent different kinds of attack.

The results of our proposed security model prove that it has the ability to detect and protect the network from different kinds of attack. But there is no guarantee that the proposed security model can detect the new attack. The proposed security model only detect some attack for secure our enterprise network.

## **6.1 Future Scope**

According to performance evaluation in figure 5.24, we observe that a firewall has a little impact on bandwidth utilization and so on network performance. We will try to use the firewall from other vendors such as Cisco ASA, we used FortiGate-3140B firewall in our proposed model. We will work to develop and implement an awareness module to be added to a proposed model. Again, we will use open source in implementing such a module, the main purpose of the module is to provide enough information about intrusions and attacks before they occur. We may need an advanced IoT based wireless security module in firewall integrate with Bluecoat devices as well as create strong policy in firewall to protect branches networks connected through wireless networks. Finally, for precision and deep log analysis, we may integrate traffic analysis with other monitoring and logging tools for demonstrate and evaluate overall network system.

## REFERENCES

- [1] Khaled W. Alnaji "Developing Security-Enhanced Model For Enterprise Network" Islamic University – Gaza Palestine 1435H (2014)
- [2] Monali S. Gaigole, Prof. M. A. Kalyankar "The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms" IJCSMC, Vol. 4, Issue. 5, May 2015, pg.728 – 735.
- [3] Brian Ritchot "An Enterprise Security Program and Architecture to Support Business Drivers" August 2013
- [4] Mr. Sachin Taluja<sup>1</sup>, Prof. Rajeshwar Lal Dua<sup>2</sup> "Survey on Network Security, Threats & Firewalls" Volume 1, Issue 7, September 2012 ISSN: 2278 – 1323
- [5] FortiGate: Next Generation Firewall (NGFW) (November 12 2018 9.24PM) is Available Here <https://www.fortinet.com/products/next-generation-firewall.html>
- [6] Richa Sharma, Chandresh Parekh "Firewalls: A Study and Its Classification" Volume 8, No. 4, May – June 2017
- [7] Sulaimon Adeniji "Network Security" Internet Technology 2012.
- [8] Binh Nguyen "Network Security and Firewall, ClearOS – A Linux Open Source Firewall" 29 April 2016
- [9] Difference between an IDS and an IPS [November 15 2018 10pm] is Available Here <https://www.pandasecurity.com/usa/support/card?id=31463>
- [10] Enhance service delivery model with WAN, application optimization [December 09 2018 8.35PM] is available here  
<https://searchnetworking.techtarget.com/definition/WAN-optimization-WAN-acceleration>.
- [11] Benefits of WAN optimization solutions [December 13 2018 7PM] is available here <https://www.riverbed.com/sg/solutions/wan-optimization.html>
- [12] Brian Ritchot "An Enterprise Security Program and Architecture to Support Business Drivers" August 2013
- [13] PORT FORWARDING AND SMALL NETWORK SECURITY [December 16 2018 11PM] available here <https://www.larrytalkstech.com/port-forwarding-small-network-security>
- [14] Active internet traffic filtering [December 19 2018 3PM] is available here <https://dl.acm.org/citation.cfm?id=1247370>
- [15] Network Access Control [December 19 2018 4PM] is available here <https://www.esecurityplanet.com/network-security/network-access-control.html>

## Appendix

### Abbreviation

LAN: Local Area Network

WAN: Wide Area Network

OS: Operating System

FTP: File Transfer Protocol

WiFi: Wireless Fidelity

SNMP: Simple Network Management Protocol

DNS: Domain Name System

IDS: Intrusion Detection System

OSI: Open Systems Interface

CD: Compact Disc

DOS: Denial-of-Service

PAD: Packet Assembler/Disassembler

ICMP: Internet Control Message Protocol

HTTP: HyperText Transfer Protocol

HTTPS: HyperText Transfer Protocol secure

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

SMLI: Stateful Multi-Layer Inspection

VPN: Virtual Private Network

IPsec: Internet Protocol Security

UFO: Uncompleted Firewall

APT: Advanced Persistent Threat

MITM: Man in the Middle

VLAN: Virtual Local Area Network

CAM: Content Addressable Memory

MAC: Media access control

STP: Spanning Tree Protocol

ARP: Address Resolution Protocol

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

DDoS: Distributed Denial of Service  
MITM: Man in the Middle  
PPTP: Point-to-Point Tunneling Protocol  
MPLS: Multiprotocol Label Switching  
MLS: Multi Level Security  
ESP: Encapsulating Security Payload  
AH: Authentication Header  
IKE: Internet Key Exchange  
TLS: Transport Layer Security  
PIN: Personal Identification Number  
SMTP: Simple Mail Transfer Protocol  
DAS: Discretionary Access Control  
ITF: Internet Traffic Filtering  
NAC: Network Access Control  
NAT: Network Address Translation  
ACL: Access Control List  
GNS3: Graphical Network Simulator-3  
CLI: Command Line Interface  
ARP: Address Resolution Protocol  
VM: Virtual Machine  
IETF: Internet Engineering Task Force  
ASA: Adaptive Security Appliance  
CPU: Central Processing Unit