Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 10, October 2019, pg.109 – 122

A Framework of Wireless Network Security Threats: Solution for Various Information Security Problems

Najiya Sultana
Assistant Professor, Dept. of Computer Science & Engineering, Taibah University, Al-Madina Munawara, KSA
najiya.research@gmail.com

Abstract: ***The principles of security threats prevent inappropriate access, modification or manipulation of data from taking place. The chapter focuses on Information security threats principle components as well as the security. The comprehensive model for information security is also discussed here very briefly. Finally, this chapter focuses on information security system and the various implementation phases. In this chapter mainly different areas are discussed such as Information Security and Critical characteristics of information in Mobile Ad-hoc Networks.***
Keywords: ***Firewall, Threat Analysis, Information, Security, Mobile Ad-hoc Networks, Intrusion Detection Systems.***

I. INTRODUCTION

The principles of security threats prevent inappropriate access, modification or manipulation of data from taking place. The chapter focuses on Information security threats principle components with human computer interaction as well as the security. The comprehensive model for information security is also discussed here very briefly. Finally, this chapter focuses on information security system and the various implementation phases. In this chapter mainly different areas are discussed such as Information Security and Critical characteristics of information.

II. BACKGROUND

Internet is the worldwide collection of network which is loosely connected, so that it can easily be accessible by any host in a variety of ways. The main risk here is that any valuable information can be lost, stolen, changed or

misused. After the complete review of the chapters, we will learn about information security and become familiar with various techniques.

III. The History of Security Threats in Information

Military commanders and every individual user thought that it was necessary to protect the data from unauthorized users. And hence this can be enforced by providing confidentiality of information and also we need various means to detect tampered message but better protection could be achieved through the various protocols. Any sensitive information is considered to be most important and protected against untrusted persons, and kept in a more secured environment or high box.

In 1889, the British Government published the Official Secrets Act. At the time of World War, the classification system like multitier was commonly used to communicate information to and from various fronts; this encouraged to use the code breaking sections. The Government Code and Cipher School is been created in United Kingdom in the year 1919. During those days, encoding had become more difficult between the wars as many computer machines were been used to scramble and unscramble information. At the time the Second World War, the information was shared by the allied countries that were required for formal alignment of classification systems and procedurals controls.

By the end of 20th century and the beginning of 21st century, we had seen advancement in various fields like telecommunication, software, hardware and encryption of data. From a business to the home user, all were exposed to many powerful and less expensive computing devices that made electronic data processing very easy. At the same time, all these devices are been interconnected by Internet.

IV. WHAT IS SECURITY?

The steps that are taken to secure organization information depend on various circumstances. it should impose multiple layers of security at different places to protect the system.

It also deals with the protection of data from physical circumstances and also from various events that could cause loss or damage to an institution or agency. It also deals with the protection from fire, natural disasters and terrorism.

Personal Security

Personal security is the protection of a person who is authorized to access organization and its operation.

Network Security

Network security deals with providing security to network components and also the connections.

V. INFORMATION SECURITY PRINCIPLES

Information is known to be an asset to all individuals and businesses. An asset can be documents; data is identified with three main characteristics:

- It can be created, processed and used to store, it can be transmitted, destroyed, sometimes corrupted or lost.

Info Security model shown in figure 1.1.

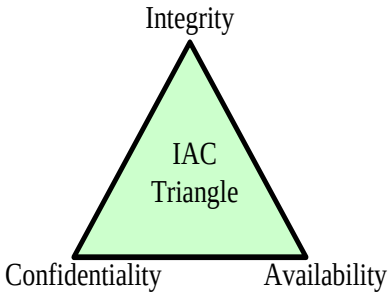

Figure 1.1 Security Principles

The I.A.C triangle is considered this concept.

McCumber Cube

McCumber Cube is the model to develop a secure system. It not only considers key security goals like CIA model, but it should also address about how goals relate to other various states in which information resides. And at the same time address the full range of available security measures

McCumber Cube is for establishing and evaluating information security programs.

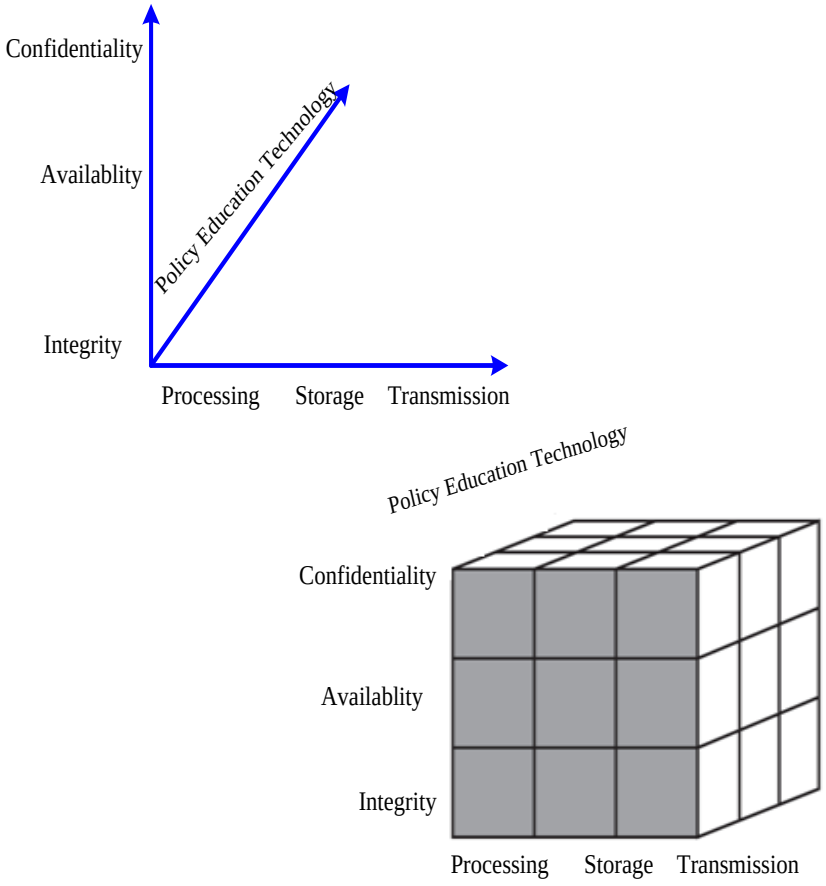

Fig. 1.2 Security Model for NSTISSC

The X axis represents various Information States:-

- Storage state - 'data at rest', such as data stored in memory or on a disk
- Transmission state - 'data in transit' - data being transferred between systems, in physical or electronic form
- Processing state - data being actively examined or modified

The Y axis represents Security goals: As discussed with the C.I.A model.

The Z axis represents Countermeasures/Safeguards

- Technology safeguard- software and hardware solutions (e.g., antivirus, firewalls, intrusion-detection systems, etc.)
- Policy and practices protection- administrative controls, such as management directives (e.g., acceptable use policies)
- People safeguard - aka awareness, training, education

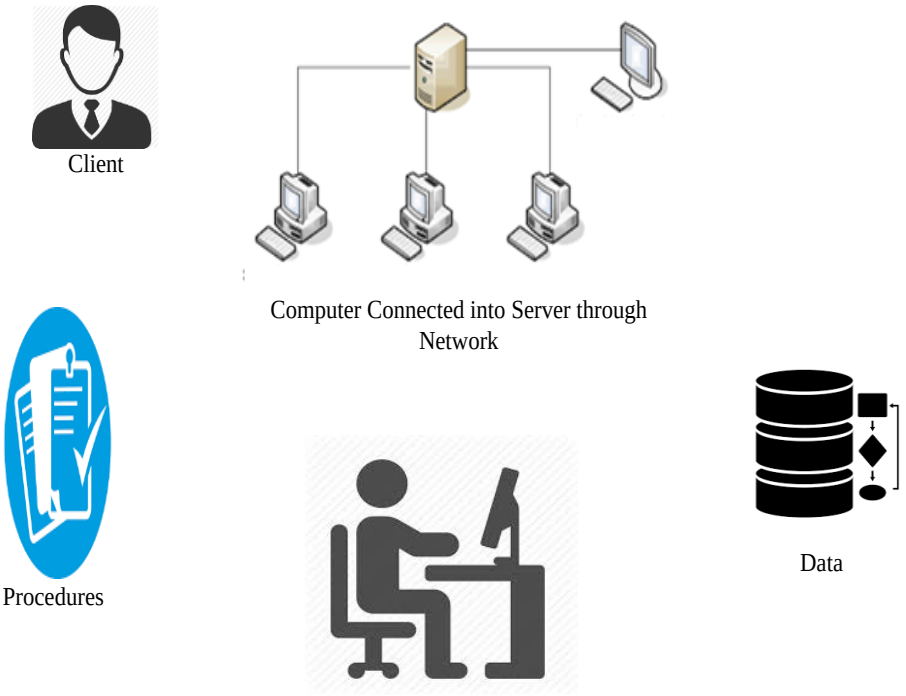

Fig 1.3 Components for Information System

We refer to the parts of computers, the tools used for physical security are locks and keys; these tools impose certain restrictions in accessing and interacting equipment.

People

People are human. So, People are always considered as a primary threat to information security.

Procedures

Procedures are information.

Networks

Today, computer systems are usually interconnected by various types of networks. Every person as access to the internet and has the own network. Therefore, security is must for networks to protect them from hijacking and other things that can damage the networks. As we know that computer networks and internet is very important for us, therefore it must be secure.

VI. APPROACHES TO INFORMATION SECURITY IMPLEMENTATION

A system consists of many components. The abstraction of higher layer can be achieved until the last stage is reached where few activities are only supported by layers that are required by the system. Protection referred to as security systems development life cycle (Sec-SDLC). To understand Sec-SDLC we need to know the basics of SDLC.

1. Investigation

During this phase, we conduct a preliminary analysis, to find out the organization's purpose, nature and scope of the problem. We can study about how the problem will fit them.

A feasibility study should be conducted before any system planning, as shown in figure 1.4. This can help in determining the conclusion of this phase.

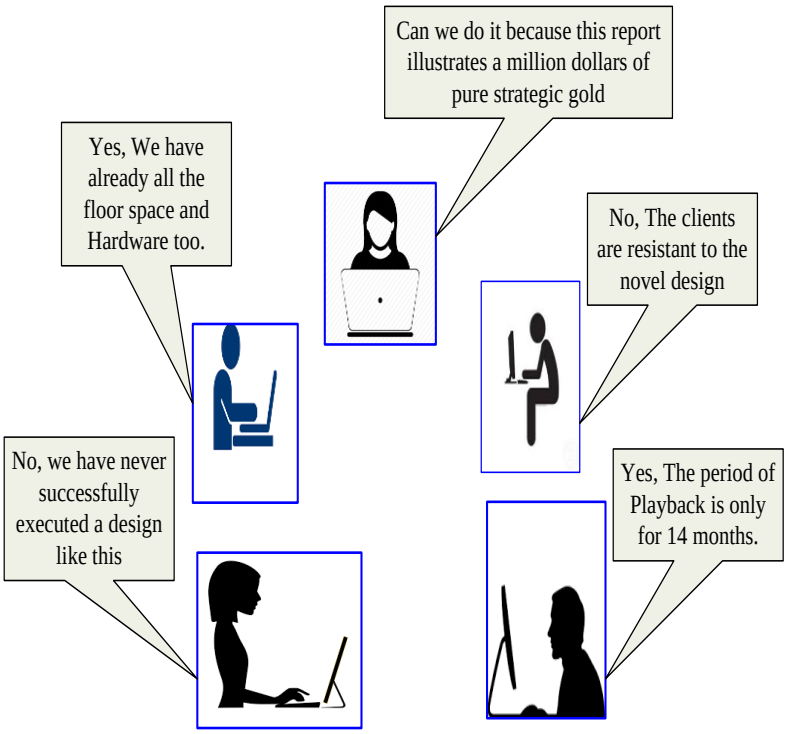

Fig 1.4: Feasibility Analysis

2. BLUEPRINTS FOR BUILDING AN INFORMATION SECURITY PROGRAM

2.1 INFORMATION SECURITY BLUEPRINTS

The framework is a "blueprint" for building an information security program. Framework can solve various information security problems, like building blueprints to meet their required specifications. Management must decide to proceed or not with the development of the Blueprint. With framework as the basic skeletal structure, detailed planning of the Blueprint can be developed.

Every implementation might require modification.

There are a number of published information security frameworks:

2.1.1 The ISO 27000 Series

Information technology is commonly used security model; it supports (ISO) and (IEC) as ISO/IEC 17799 both were been adopted as international standards, as a framework for information security.

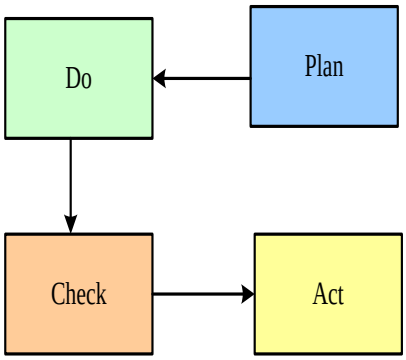

Figure 2-1: Plan-Do-Check-Act

3. TECHNOLOGY- FIREWALLS

3.1 OVERVIEW

It helps us to various approaches to firewall implementation. You will understand about content filtering technology.

3.2 OBJECTIVES

- Understand the various Firewall Architecture and types of Firewalls.
- Understand how to select the right firewall for an organization

3.3 FIREWALLS

Every user who connects their computers to the external world like the internet must be aware of attacks and know how to protect their data. When connected to the internet, the confidential data are easily exposed to malicious attack anywhere in the world and make easy targets for malicious software & dishonest hackers.

3.4 WHAT ARE FIREWALLS

A firewall act as network security is defined as a software program that prevents hackers, worms and viruses attack. It implemented on the network perimeter, and function by defining trusted and untrusted zones as shown in Figure 3.1.

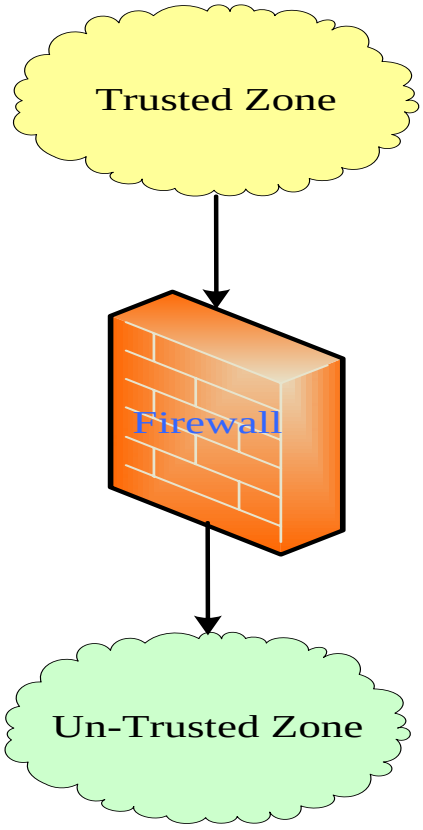

Figure 3.1 Firewall Device

The firewall control traffic flow between trusted zone and untrusted zone. They are available as stand-alone products and sometimes found in broadband routers. Software firewalls are programs installed on computers. The software program can be customized by enabling some control on protection features. Software firewall protects the system from being accessed by external entities.

Firewall disables the access to different parts of a network. Most of the time, they are found in the private network.

Firewalls are implemented by certain "security rules". Rules can be set up by the system administrator or computer owner that allows valid traffic to make access to servers like web servers, FTP servers, telnet servers, etc.

All traffic that flows between inside and outside network are controlled and monitored by firewalls. They decide what kind of connections can be made.

3.5 FIREWALLS CLASSIFICATION

3.5.1 There are various types of firewall technologies. Among them, let us now take a quick review of each and provide an overview about different firewall technologies.

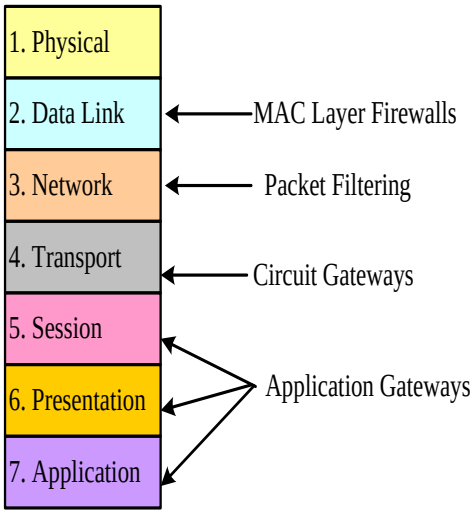

Figure 3-2: Firewall Types and OSI model

3.5.2 Packet-filtering firewalls (Filtering Firewall)

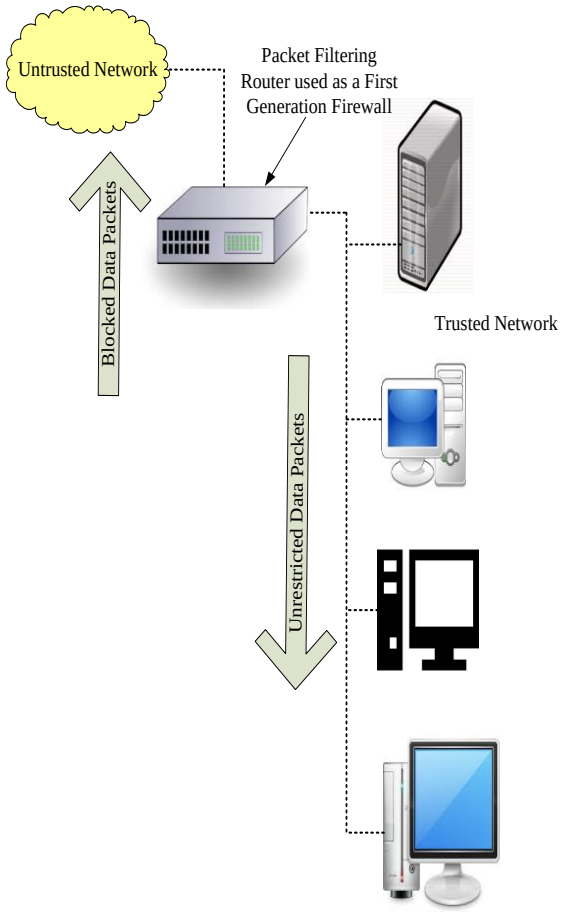

Figure 3-3: Packet Filtering Router

The Packet Filtering firewall examines packets. Firewalls network layer examine whether to drop or allow a packet. Packet filters are useful in any perimeter security setup. A Packet also called as datagram's consist of the header part and the data part. Packet header part is used to decide whether to block the packet or allow it to pass through a firewall.

Packet-filtering router, as shown in the Figure, is used to filter data packets by examining incoming and outgoing connections. They restrict unauthorized access to a public network.

It finds out the packets that violate the firewall rules. There are certain restrictions implemented on packet filtering firewalls. They also enforce address restrictions. If the device found any packet, that maps to this restrictions than it denies those packets from entering the network.

Packet filtering firewalls are classified into three subtypes.

- In dynamic filter firewall rules are defined based on an event dynamically. It denying packets based on information in packet header.
- Stateful inspection: These types of firewalls are called as Stateful firewalls.

3.5.3 Gateway

The proxy server will access the Web server and return the requested page to a user.

3.6 CIRCUIT GATEWAY

The Circuit gateway always functions at the transport layer. The circuit gateway firewalls can examine all packets and it will allow or block packets in a TCP or UDP connection. It avoids direct connections between networks and creates tunnels. They support virtual private network across the Internet and helps in encryption between firewalls.

3.6.1 MAC Layer Firewall

MAC layer firewalls map the MAC address to Access control list to allow or block the packets.

3.6.2 Hybrid Firewall

Hybrid firewalls combine the different types of firewalls, like packet filter with application or packet firewall with circuit gateway. Often hybrid firewalls are designed with two firewall devices, were both will operate in parallel.

3.6.3 Firewalls Categorized by Generation

Michael Gregg is the security expert has divided firewalls into generations.

- **1 Generation**: Are static packet-filtering firewalls. These firewalls filter the packet by examining the packet header.
- **2 Generation**: These firewalls are a request.

3.6.4 Firewalls Categorized by Structure

Based on the structure to implement firewalls are categorized as follows:

- **Firewall Commercial Appliance**

  Firewall Commercial Appliance is similar to the computer with additional firmware based instructions.

- **Firewall Software**

  The software can run on any general-purpose computer. Most of the time organizations purchase hardware as per the required specification and install this application software. This firewall gives optimum performance.

- **Firewall Residential Appliances**

  These firewalls are Small Office Home Office firewall devices. These devices are used in LAN. A residential user most often uses this type of firewall. A firewall can be installed. The most common example is McAfee Internet Security, Norton Internet Security, etc.

3.7 FIREWALL ARCHITECTURES

Firewalls are always implemented by Different firewall components when grouped together, four most common types of firewall architectures exist like:

The packet filtering router is simplest form among all types. These filters are implemented as shown in the Figure 3-7. Router is placed in trusted network/Untrusted network internet connection. Routers route traffic from one interface to other. Routers are configured to allow or reject packets that the organization wants by defining the security rules. If something is wrong with the router, then unauthorized traffic can easily enter the trusted network.

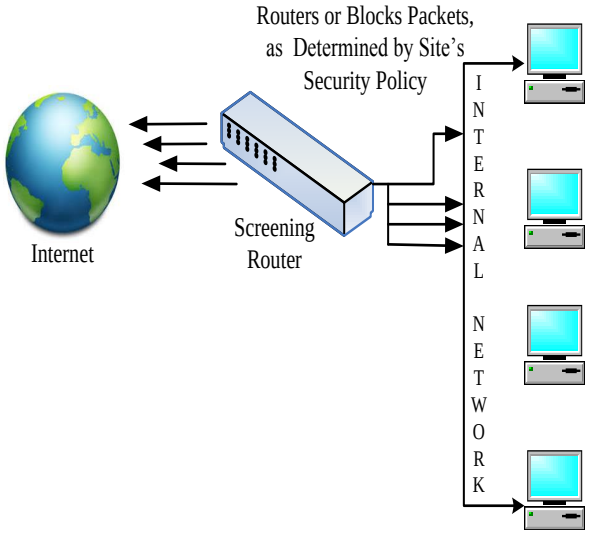

Figure 3-7: Packet Filtering Firewall

The advantage is they are completely transparent to all parties involved in the network. Packet filtering protects an entire network with a single router. With one router, you can connect the internal network to the internet. The drawback is the single point of failure. The system lacks auditing and strong authentication. Packet filtering will create heavy load on a router, and this can degrade the router performance.

3.7.1 Screened Host Firewalls

It is also called as Bastion Host as shown in Figure 3.8. A bastion host is present in the internal network. The external host should connect to Bastion host in the internal network for any required service. Bastion host can be considered as the defender at the network perimeter, so also called as sacrificial host.

The advantage of this architecture is it gives best safety than packet filtering router. The drawback of the screened host architecture is if the attacker tries to break into bastion host; then internal network security is completely lost. Packet filtering router can lead to single point failure. If attacker attempts to compromise the router, then the entire network will be easily accessible to attackers.

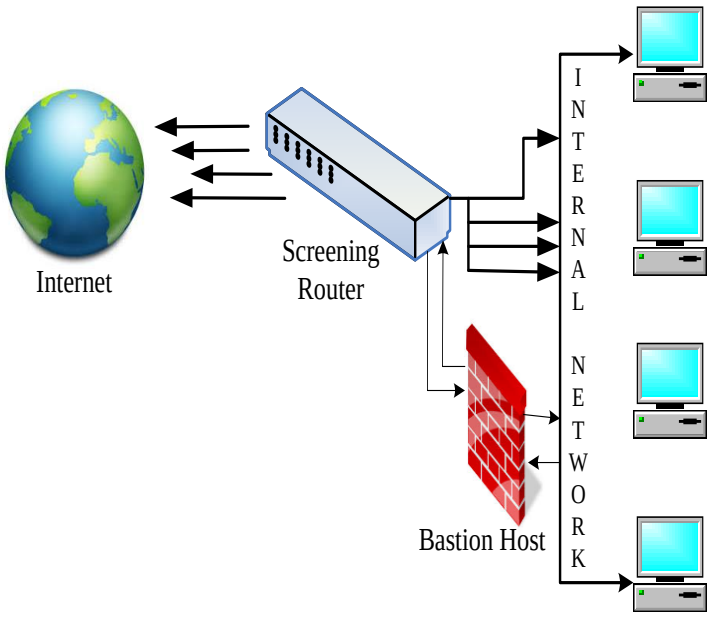

Figure 3-8: Screened Host Firewall

3.7.2 Dual-Homed Firewall

Dual-Homed Firewall architecture is designed by placing a dual-homed host as shown in the Figure 3-9.

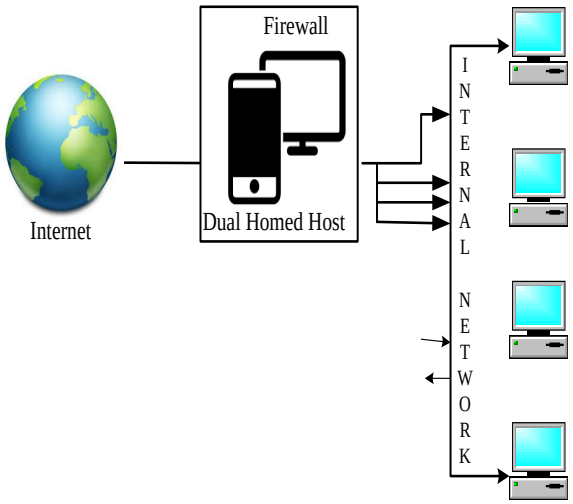

Figure 3-9: D-H H Firewall

Dual homed host will exist as a router between networks to route IP packets. All traffic must go through the firewall with two NICs. The implementation of this architecture requires NAT. NAT shows external IP address to internal IP address; thereby it can avoid intrusion from external attackers. The advantage of this firewall is simple and more robust than Packet filtering router.

3.7.3 Screened Subnet Firewalls (with DMZ)

Screened subnet firewall is slight variation of the dual-homed gateway and screened host firewall. In this architecture, DMZ (Demilitarized Zone) is created. The DMZ is the less restricted area with a dedicated port on the firewall device, as shown in Figure 3-10.

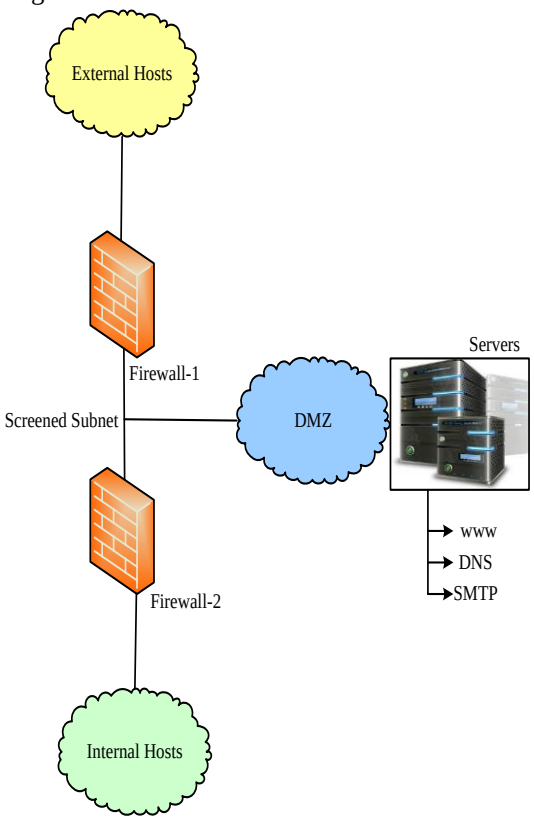

Figure 3-10: Screened Subnet Host Firewall

There are three interfaces. The first interface is the public interface and connects to the External Hosts (Internet). Second Interface connects to DMZ to which public services like WWW, DNS, SMTP, etc., are attached. The third interface connects to internal Hosts. Connections from the external host to internal hosts are routed through Firewall 1. Connections from the internal host to external hosts are routed through Firewall 2.

3.8 MANAGEMENT OF FIREWALL

There are certain questions that arise while selecting a firewall.

- Which type of firewall technology?
- What features are supported with the firewall of actual price?
- How to configure the firewall?

3.9 FIREWALL RULES

Best practices for firewalls

Firewalls rules can be framed depending on the needs, requirements & security threat levels. As and when required firewall rules can be created or disabled based on few conditions like IP Addresses, Ports and Keywords. Firewall rules are set by firewall administrator based on certain predetermined rules. A firewall examines every data packet by comparing it against firewall rules framed.

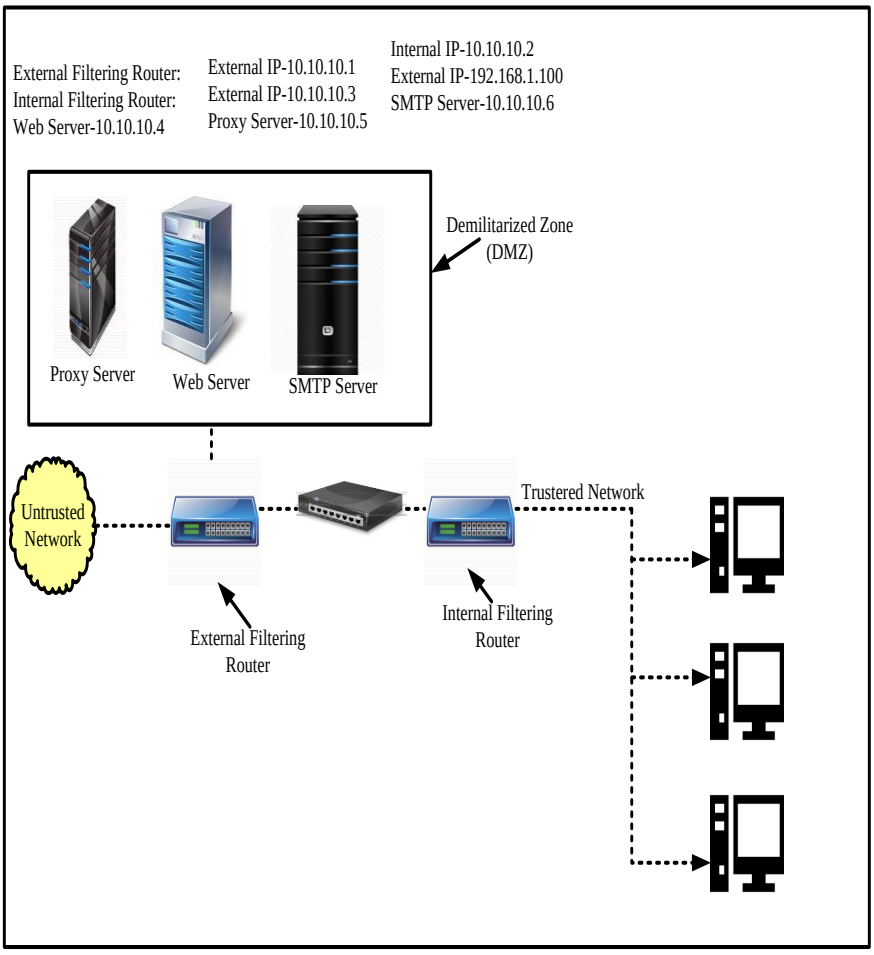

Figure 3-11: Example Network Configuration

VII. CONCLUSION

Filtering firewalls can be implemented as static filtering, dynamic filtering, and Stateful inspection firewalls. Firewalls are often categorized by the generation of the technology with which they are implemented, which ranges from the first to the fifth generations. Firewalls can be categorized by the structural approach used for the implementation, including commercial appliances, commercial systems, residential/SOHO appliances, and residential software firewalls. Content filtering can improve security and assist organizations in improving the manageability of the use of technology. Firewalls operate by evaluating data packet contents against logical rules.

Query (the questions that are addressed in this chapter)

1. Explain categories of firewalls based on processing mode.
2. Explain categories of firewalls based on Development Era and Structure.
3. How a firewall can be configured and managed?
4. Explain the FIREWALL RULES
5. Explain Content Filters

REFERENCES

[1]. http://www.cisco.com/networkers/nw04/presos/docs/SEC-1N20.pdf Accessed on 12-06-14
[2]. https://www.freebsd.org/doc/handbook/firewalls.html#firewalls-intro accessed on 12-06-2014
[3]. http://www.routeralley.com/ra/docs/intro_firewalls.pdf accessed on 11-06-2014
[4]. http://microboss.com.au/broadband/firewall_architecture.pdf accessed on 16-06-2014
[5]. http://www.invir.com/int-sec-firearc.html
[6]. http://www.symantec.com/connect/articles/introduction-ids accessed on 18-6-2014
[7]. http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
[8]. http://www.idt.mdh.se/kurser/ct3340/ht09/ADMINISTRATION/IRCSE09-submissions/ircse09_submission_18.pdf
[9]. http://www.pcporoje.com/filedata/947354.pdf
[10]. http://vlsi.byblos.lau.edu.lb/classes/csc736/handouts/Intrusion-Detection-Intro.pdf
[11]. http://www.ijarcsse.com/docs/papers/8_August2012/Volume_2_issue_8/V2I800201.pdf accessed on 20-06-2014
[12]. http://en.wikipedia.org/wiki/Intrusion_detection_system
[13]. http://www.symantec.com/connect/articles/wireless-intrusion-detection-systems
[14]. http://www.cs.illinois.edu/~caesar/courses/CS598.S13/slides/philip_IDS_practice.pdf
[15]. http://www.cse.hcmut.edu.vn/~ttqnguyet/ISSecurityForMIS_2011/slide10_IDPSystem.pdf
[16]. http://airccse.org/journal/nsa/0313nsa08.pdf
[17]. http://www.tracking-hackers.com/papers/honeypots.html

