

We approve the thesis of Metin TOK

# A Firewall Design For Academic Environments

Date of Signature



Asst. Prof. Dr. Ahmet KOLTUKSUZ

by  
Metin TOK

Supervisor

Department of Computer Engineering

28 / 06 / 2001

## A Dissertation Submitted to The Graduate School in Partial Fulfillment of The Requirements For The Degree of



Asst. Prof. Dr. Tuğhan TUĞLULAR

Department of Computer Engineering

28 / 06 / 2001

### MASTER OF SCIENCE



Asst. Prof. Dr. Levon

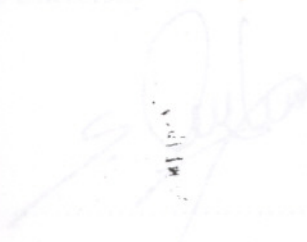
Department: Computer Engineering

Department of Computer Eng

Major: Computer Software

28 / 06 / 2001

Eye Unit



Prof. Dr. Sali

Head of Department

**İzmir Institute of Technology**  
İzmir, Turkey

June, 2001

İZMİR YÜKSEK TEKNOLOJİ ENSTİTÜSÜ	
REKTÖR	
Kütüphane ve Dokümantasyon	
Bölge Başkanı	
Ders No:	720
Yıl No:	1999-2000
Geliş Tarihi:	

## ACKNOWLEDGEMENT

We approve the thesis of **Metin TOK**

First, I would like to thank to my advisor *Assoc. Prof. Dr. Ahmet KOLTUKSUZ* for advices and for his patience when I write this thesis.

**Date of Sinature**

Many thanks to *TYTE, Computer Application & Research Center and Department of Computer Engineering.*

And many thanks to *Turkish Air Force MEBS School Commander to let me*  
..... *in TYTE.*



**Assoc. Prof. Dr. Ahmet KOLTUKSUZ**

Supervisor

Department of Computer Engineering

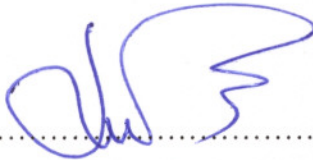
28 / 06 /2001



**Asst. Prof. Dr. Tuğkan TUĞLULAR**

Department of Computer Engineering

28 / 06 /2001

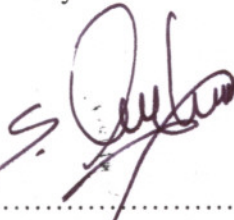


**Assoc. Prof. Dr. Levent TOKER**

Department of Computer Engineering

Ege University

28 / 06 /2001



**Prof. Dr. Sıtkı AYTAÇ**

Head of Department

28 / 06 /2001

## ACKNOWLEDGEMENT

First, I would like to thank to my advisor *Assoc. Prof. Dr. Ahmet KOLTUKSUZ* for advices and for his patience when I write this thesis.

Many thanks to IYTE, Computer Application & Research Center and Department of Computer Engineering.

And also, many thanks to Turkish Air Force MEBS School Commander to let me continue the Master of Science in IYTE.

## ABSTRACT

Computer networks in academic environments could have many security problems if there weren't enough precaution. The source of these problems is generally vulnerabilities of TCP/IP protocol and Internet. Vulnerabilities can cause threats. These threats will be analyzed in this thesis. There are many kind of countermeasures to prevent the assets of the academic networks. Firewalls are a kind of countermeasure against these attacks. In this thesis, these countermeasures will be also analyzed and a firewall will be designed and proposed for academic environments against these threats.

## ÖZ

Akademik ortamların bilgisayar ağlarının birçok güvenlik problemi bulunmaktadır. Bu problemler genellikle TCP/IP protokolundan ve İnternette kaynaklanmaktadır. Bu tezde bu problemler analiz edilecektir. Akademik ortamların bilgisayar ağlarının değerli nesnelere korumak için birçok tedbir vardır. Firewall'lar, bu tehditlere karşı alınabilecek önlemlerden biridir. Bu tezde bu önlemler analiz edilecek ve bu tehditlere karşı akademik ortama uygun bir firewall tasarlanacak ve önerilecektir.

## TABLE OF CONTENTS

LIST OF FIGURES .....	x
LIST OF TABLES .....	xi
CHAPTER 1 INTRODUCTION .....	1
1.1 Purpose .....	1
1.2 Scope .....	2
1.3 Organization .....	2
CHAPTER 2 OVERVIEW OF NETWORK AND INTERNET SECURITY .....	3
2.1 Basic Security Concepts .....	3
2.2 Threats Against The Network Security .....	4
2.3 Security Policy and Procedures .....	4
2.4 Security Technology .....	4
2.4.1 Firewalls .....	4
2.4.2 Intrusion Detection Tools .....	4
2.4.3 Security Analysis Tools .....	5
2.4.4 Cryptography .....	5
2.4.4 Authentication Tools .....	5
CHAPTER 3 FUNDAMENTAL OF FIREWALLS .....	6
3.1 Firewall Technologies .....	6
3.1.1 Packet filters .....	6
3.1.2 Network Address Translation (NAT) .....	7
3.1.3 Proxy filters .....	8
3.1.4 Hybrid Firewalls .....	9
3.2 Firewall Architectures .....	10
3.2.1 Screening Router (Packet Filter) .....	10
3.2.2 Dual-Homed Host .....	11
3.2.3 Screened Host .....	11
3.2.4 Screened Subnet .....	12
CHAPTER 4 THREATS FOR NETWORK SECURITY .....	13
4.1 Some Statistics About Security Incidents .....	13
4.2 Port Scanning .....	13
4.3 Packet Sniffers .....	14
4.4 IP Spoofing .....	14

4.5 Denial of Service .....	15
4.5.1 TCP SYN Flood .....	15
4.5.2 Ping of Death .....	16
4.5.3 Smurf Attack .....	16
4.5.4 UDP Port Denial-of-Service Attack .....	16
4.5.5 Email Bombing and Spamming .....	16
4.6 Password Attacks .....	17
4.7 Man in the Middle Attacks .....	17
4.8 Hijacking .....	17
4.9 Predicting TCP Initial sequence numbers .....	17
4.10 Replay Attack .....	18
4.11 Application Layer Attacks .....	18
4.12 Network Scanners .....	18
4.13 DNS Security Problems .....	19
4.14 Trust Exploitation .....	19
4.14 Port Redirection .....	19
4.15 Unauthorized Access .....	19
4.16 Virus and Trojan Horse Applications .....	20
4.17 Remote Procedure Call (RPC) .....	20
4.18 Insiders .....	20
<b>CHAPTER 5 COUNTERMEASURES AGAINST THREATS .....</b>	<b>21</b>
5.1 Port Scanning .....	21
5.2 Packet Sniffers .....	21
5.3 IP Spoofing .....	21
5.4 Denial of Service .....	23
5.4.1 TCP SYN Flood .....	23
5.4.2 Ping of Death .....	24
5.4.3 Smurf Attack .....	24
5.4.4 UDP Port Denial-of-Service Attack .....	24
5.4.5 Email Bombing and Spamming .....	25
5.5 Password Attacks .....	25
5.6 Man-in-the-Middle Attacks .....	25
5.7 Hijacking .....	25

5.8 Predicting TCP Initial sequence numbers .....	26
5.9 Replay Attack .....	26
5.10 Application Layer Attacks .....	26
5.11 Network Scanners .....	27
5.12 DNS Security Problems .....	27
5.13 Trust Exploitation .....	27
5.14 Port Redirection .....	27
5.15 Unauthorized Access .....	28
5.16 Virus and Trojan Horse Applications .....	28
5.17 RPC .....	28
5.18 Insiders .....	28

## CHAPTER 6 ASSETS AND NEEDS OF ACADEMIC

ENVIRONMENT NETWORK .....	30
6.1 Electronic Mail .....	30
6.2 Network News Transfer Protocol (NNTP) .....	30
6.3 Real Time Conferencing Services .....	30
6.4 World Wide Web (WWW) .....	31
6.5 File Transfer (FTP, TFTP) .....	31
6.6 NFS .....	31
6.7 Domain Name Servers .....	31
6.8 Password and Key Servers .....	32
6.9 Routers .....	32
6.10 Firewalls and Intrusion Detection Systems (IDS) .....	32
6.11 Remote Access .....	32
6.12 Information Transactions .....	33
6.13 High Availability .....	33
6.14 Ease of Use .....	33
6.15 Openness .....	34

## CHAPTER 7 CASE STUDY: FIREWALL DESIGN FOR IYTE .....

7.1 Design Principles .....	35
7.1.1 Least privilege .....	35
7.1.2 Defense in Depth .....	35
7.1.3 One Gate .....	35
7.1.4 Weakest Link .....	35



7.1.5 Information Sharing .....	35
7.1.6 Simplicity .....	35
7.2 Countermeasures and Assets Decision Table .....	36
7.3 Constitution The Firewall Rules .....	41
7.4 Components of IYTE Firewall .....	51
7.4.1 HTTP Server .....	51
7.4.2 Mail Server .....	51
7.4.3 Telnet .....	51
7.4.4 SSH Server .....	52
7.4.5 FTP .....	52
7.4.6 NNTP Server .....	52
7.4.7 Authentication Server (Kerberos) .....	52
7.4.8 DNS Server .....	52
7.4.9 Packet Filtering Rules .....	53
7.4.10 Interior Firewall .....	53
7.4.11 Exterior Firewall .....	53
7.5 Need of Authentication and Privacy .....	53
7.6 Need of Intruder Detection System .....	54
7.7 Need of Testing Firewall .....	54
CHAPTER 8 CONCLUSION .....	55
SUMMARY .....	56
ÖZET .....	57
BIBLIOGRAPHY .....	58

## LIST OF FIGURES

Figure 3.1 Incoming Packet Filtering Algorithm .....	6
Figure 3.2 Outgoing Packet Algorithm .....	7
Figure 3.3 Network Address Translation (NAT) .....	8
Figure 3.4 Proxy Filter .....	9
Figure 3.5 Packet Filter Firewall .....	10
Figure 3.6 Dual Homed Host Firewall .....	11
Figure 3.7 Screen Host Firewall .....	11
Figure 3.8 Screened Subnet Firewall .....	12
Figure 5.1 RFC 2827 Filtering .....	22
Figure 7.1 Network Infrastructure of IYTE Campus .....	42
Figure 7.2 Firewall Implementation-A for IYTE Campus .....	43
Figure 7.3 Firewall Implementation-B for IYTE Campus .....	44
Figure 7.4 Detailed View of Firewall-A .....	45

## LIST OF TABLES

Table 7.1 Firewall Rule Decision Table .....	36
Table 7.2 IP Filter Configuration of Interior Hybrid Firewall .....	46
Table 7.3 IP Filter Configuration of Interior Hybrid Firewall .....	49

İZMİR YÜKSEK TEKNOLOJİ ENSTİTÜSÜ  
REKTÖRLÜĞÜ  
Kütüphane ve Dokümantasyon Daire Bşk

## Chapter 1

### INTRODUCTION

#### 1.1 Purpose

It cannot be imagined an academic environment without information and communication. Today, Internet is the main source of information. Unfortunately, Internet is based on TCP/IPv4 protocol suite. TCP/IPv4 protocol was originally designed for openness and flexibility, not for security. Although the Internet was originally conceived of and designed as a research and education network, usage patterns have radically changed. The Internet has become a home for private and commercial communication besides academic environment.

In general Internet attacks based on TCP/IPv4 are quick, easy, and hard to detect and trace. An intruder does not have to be physically present to carry out the attack. In fact, many attacks can be launched readily from anywhere in the world and the location of the intruder can easily be hidden. Hence, security requirements are main consideration while connecting Internet.

Each site has different security level and openness need. Academic environments also have different security needs from a military site. Each site needs a framework for making specific decisions, such as which defense mechanisms to use and how to configure services and procedures for users and system administrators to follow. This framework is called "security policy". Organizations determine their security policies according to their needs.

There is a generally accepted approach in developing a security policy for any site. This includes the following steps<sup>1</sup>:

1. Identify what you are trying to protect.
2. Determine what you are trying to protect.
3. Determine how likely the threats are.
4. Implement measures which will protect your assets in a cost- effective manner.
5. Review the process continuously and make improvements each time a weakness is found.

Without a fundamentally secure infrastructure, defending the network becomes more difficult. Firewall is a security tool which protects systems and information against attacks. It provides a certain level of protection and they help implementing security policy at the network level.

---

<sup>1</sup> B. Fraser, "Site Security Handbook" RFC 2196,p.4

This thesis mainly focuses on design a firewall for an academic environment. But it also has some proposals about site security.

## 1.2 Scope

The scope of this thesis is to create a secure network for academic environment. Secure network includes monitoring and intruder detection systems, firewalls, policies, hardware specific securities, cryptography and network protocols. All the other participants of secure network except firewalls are beyond the scope of this thesis. More secure network protocol than TCP/IPv4 can solve most of the security problems of network. All the other protocols are also beyond of this thesis because TCP/IPv4 is de facto standard protocol.

## 1.3 Organization

The rest of this work is organized as follows.

- Chapter 2 describes background of network and Internet security.
- Chapter 3 describes fundamentals of firewalls.
- Chapter 4 describes several important threats for network security.
- Chapter 5 discusses prevention techniques against described network threats.
- Chapter 6 discusses the assets and needs of academic environment network.
- Chapter 7 presents a case study for IYTE.
- Chapter 8 presents conclusions.

## Chapter 2

### OVERVIEW OF NETWORK AND INTERNET SECURITY

In early times of computers, computers were centralized and managed in data centers. Computers were kept in locked rooms and links outside a site were unusual. Computer security threats were rare, and were basically concerned with insiders. These threats were well understood and dealt with using standard techniques: computers behind locked doors and accounting for all resources. Today, many systems are connected to the Internet which is a huge network and has no boundaries. People need to connect to the Internet to get the information. Information on the Internet can be accessed from anywhere in the world in real time. This is good for the spread of information, but easy access to information brings new risks. The risk is the security of information.

#### 2.1 Basic Security Concepts

Three basic security concepts important to information on the Internet are confidentiality, integrity, and availability. Concepts relating to the people who use that information are authentication, authorization, and nonrepudiation.

When information is read or copied by someone not authorized to do so, the result is “loss of confidentiality”. Confidentiality is a very important attribute for some types of information such as military secrets, new product specifications, etc.

Information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is “loss of integrity”. This means that unauthorized changes are made to information by human error or intentional tampering. Integrity is particularly important for air traffic control data, financial data and etc.

Information can be erased or become inaccessible, resulting in “loss of availability”. This means that people who are authorized to get information cannot get what they need. Availability is often the most important attribute in service-oriented businesses that depend on information. When a user can't get access to the network or specific services provided on the network, they experience a “denial of service”.

To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. “Authentication” is proving that a user is who he or she claims right person by using password, smartcard, fingerprint or etc. “Authorization” is the act of determining whether a particular user or computer has the right to do a certain activity, such as reading a file or running a program. Users must be authenticated before doing the activity they are authorized to perform. “Nonrepudiation” means not to be refused authentication later. The user cannot later deny that he or she performed the activity.

## 2.2 Threats Against The Network Security

A network security threat is any network related activity with negative security implications. This usually means that the activity violates security policy. Threats come in all shapes and sizes. They can come from anywhere on the Internet, although some attacks must be launched from specific systems or networks and some require access to special accounts. The main cause of the threats is vulnerabilities of network. Many early network protocols such as TCP/IP was designed without security in mind. Without a fundamentally secure infrastructure, network defense becomes more difficult. Types of threats are explained in subsequent chapters.

## 2.3 Security Policy and Procedures

The main purpose of a security policy is to inform users, staff and managers of their obligatory requirements for protecting technology and information assets.<sup>1</sup> It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. The success of a security policy needs educated management group, improved technological support, and support of users.

## 2.4 Security Technology

A variety of technologies have been developed to help organizations secure their systems and information against intruders.

### 2.4.1 Firewalls

Intruders often attempt to gain access to networked systems by pretending to initiate connections from trusted hosts. To counter these attacks and enforce limitations on authorized connections into the organizations network, it is necessary to filter all incoming and outgoing network traffic. The firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic.<sup>2</sup>

### 2.4.2 Intrusion Detection Tools

Continuous monitoring of network activity is required to detect the intrusion. Intruder detection tool may be installed at strategic locations to collect information continuously that may indicate suspicious activity. This information may be used to find out the vulnerabilities later. It is possible to have automatic notifications alert to the system administrators when the tool detects anomalous activity. Sophisticated systems may be block suspect connections, isolate affected systems, and collect evidence for subsequent analysis.

---

<sup>1</sup> B. Fraser, "Site Security Handbook" RFC 2196,p.8

<sup>2</sup> M. Ranum , "Internet Firewalls Frequently Asked Questions", <http://www.clark.net/pub/mjr/pubs/fwfaq>

### **2.4.3 Security Analysis Tools**

It is very hard to find vulnerabilities of network by hand and it is too late after intrusion. A variety of vulnerability identification tools are available. Intruders also use these tools to detect the vulnerabilities and then intrude. These tools are useful in identifying weaknesses in systems.

### **2.4.4 Cryptography**

One of the primary reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. A well-placed network sniffer easily sees millions of electronic messages that traverse the Internet each day. Intruders may modify or give the information to others, or use it to launch an attack. One solution to this problem is to use of cryptography.

Encryption is the process of translating information from its original form (plaintext) into an encoded, incomprehensible form (ciphertext). Decryption refers to the process of taking ciphertext and translating it back into plaintext.

### **2.4.4 Authentication Tools**

Intruders often install packet sniffers to capture passwords as they traverse networks during remote login processes. Therefore, all passwords should at least be encrypted as they traverse networks. One-time password and Public Key Infrastructure (PKI) may solve this problem.



FUNDAMENTALS OF FIREWALLS

A firewall is a system or group of systems that enforces an access control policy between private network and public network. The firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic.<sup>1</sup> Firewall insulates a private network from a public network using carefully established controls. For example, an HTTP request for a public Web page will be permitted, whereas an FTP request to a host behind the firewall may not be permitted. Firewalls run a monitoring software to detect and drop external attacks on the site, and are needed to protect internal networks.

3.1 Firewall Technologies

3.1.1 Packet filters

The packet filter firewall looks through the TCP/IP header of each packet sent through it and decides whether to transmit it or not. The entire firewall operation is focused on the packet, particularly its header, which includes information such as source address, destination address, source port, destination port and direction. The algorithm is shown in Figure 3.1 and Figure 3.2.

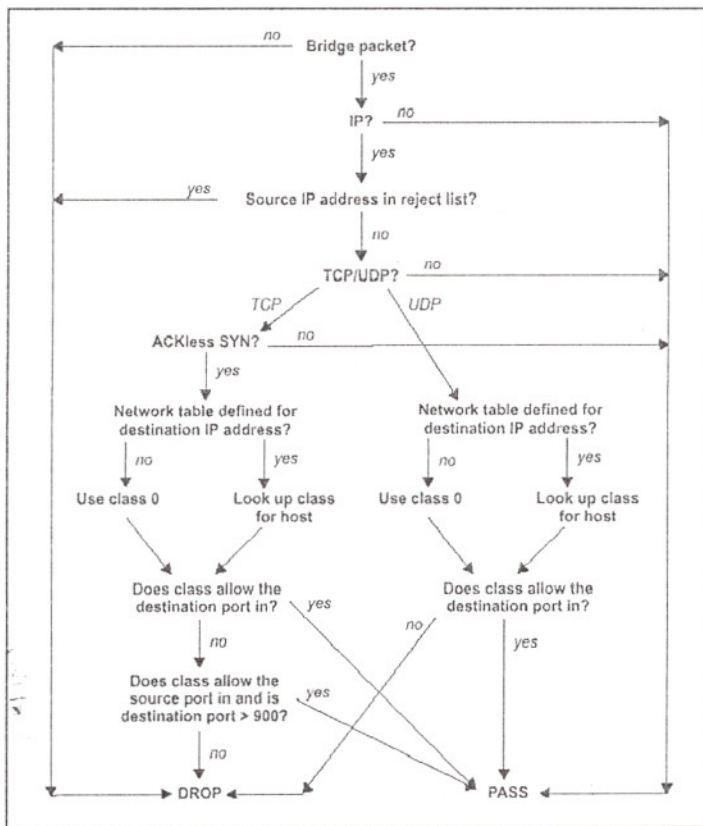


Figure 3.1 Incoming Packet Filtering Algorithm<sup>2</sup>

<sup>1</sup> M. Curtin, M. Ranum, "Internet Firewalls:Frequently Asked Questions", <http://www.clark.net/pub/mjr/pubs/fwfaq>

<sup>2</sup> D. Safford, D.Schales, D.Hess, "The TAMU Security Package", USENIX Symposium

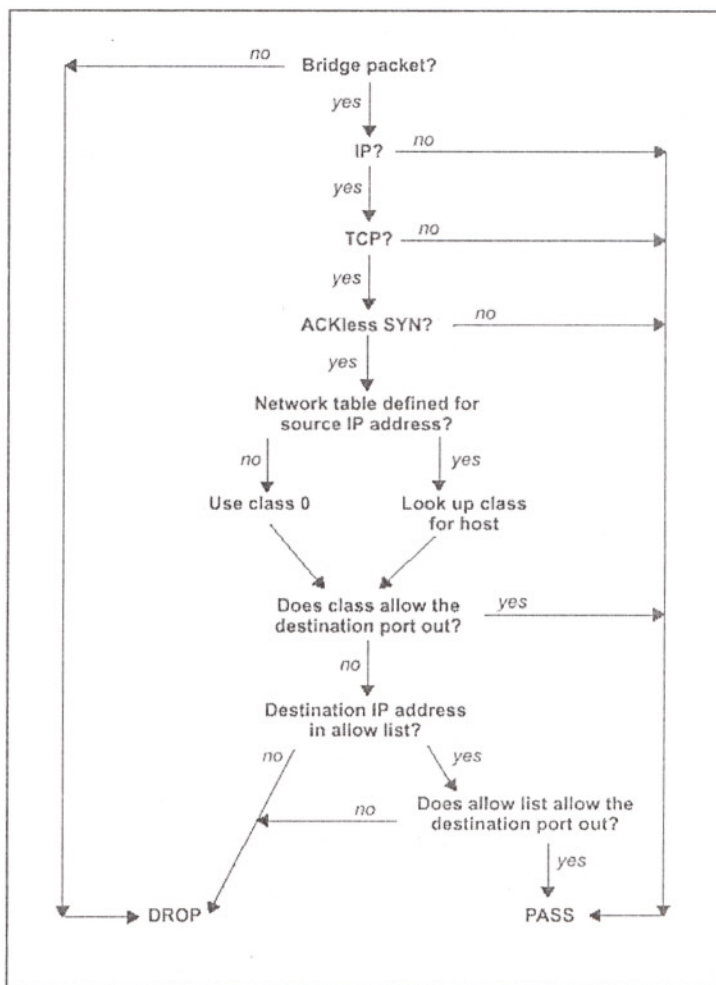


Figure 3.2 Outgoing Packet Filtering Algorithm<sup>3</sup>

In traditional packet filtering, all decisions to deny or allow packets are based on header information; no application-level information is analyzed. Because of the simplicity of their core function, packet filters tend to perform better than proxy-based firewalls. Additionally, because they sit on a connection and filter at the packet layer, they are more often than not transparent to end-users and applications.

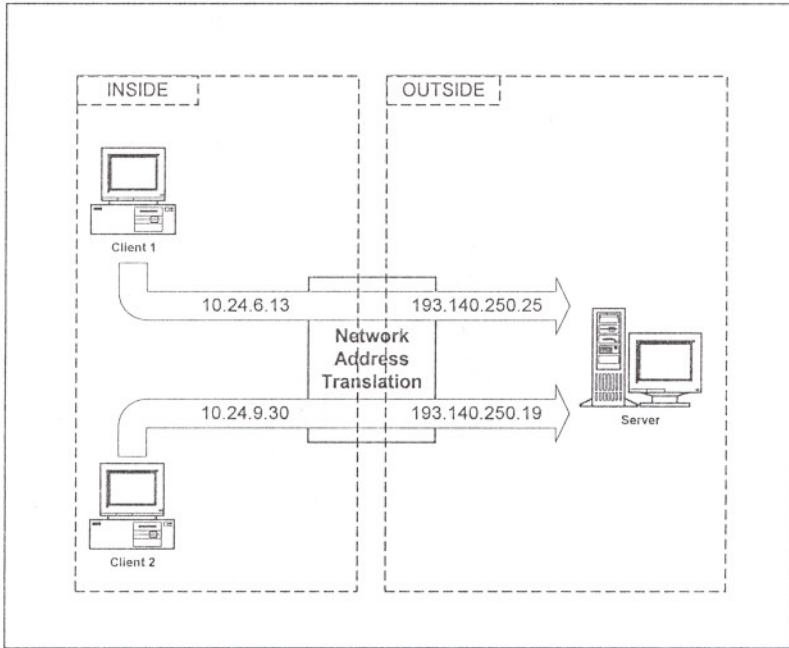
One major limitation of packet filters is their inability to understand the activities of an application. As a result, some FTP or UDP query/response services are difficult to filter. To make the process easier, some firewalls incorporate so-called "stateful" packet filters. Stateful filters increase the intelligence of the filtering process by enabling the firewall to associate some new packets with packets that were previously sent through the firewall.

### 3.1.2 Network Address Translation (NAT)

Network Address Translation (NAT) allows a network to use one set of network address internally and another set when dealing with external networks. NAT software works on a router. When an internal machine sends a packet to go outside, NAT

<sup>3</sup> D. Safford, D.Schales, D.Hess, "The TAMU Security Package", USENIX Symposium

modifies the source address of the packet to make the packet look as if in coming from a valid address, as shown in Figure 3.3. When an external machine sends a packet to go inside, NAT modifies the destination address of the packet to turn the externally visible address in to internal address.



**Figure 3.3 Network Address Translation (NAT)**

The main purpose of network address translation is to economically use address space, but it can also have security advantages. It conceals the configuration of internal network. Interfaces of routers on an internal network usually do not need to be directly accessible from outside the enterprise.<sup>4</sup>

### 3.1.3 Proxy filters

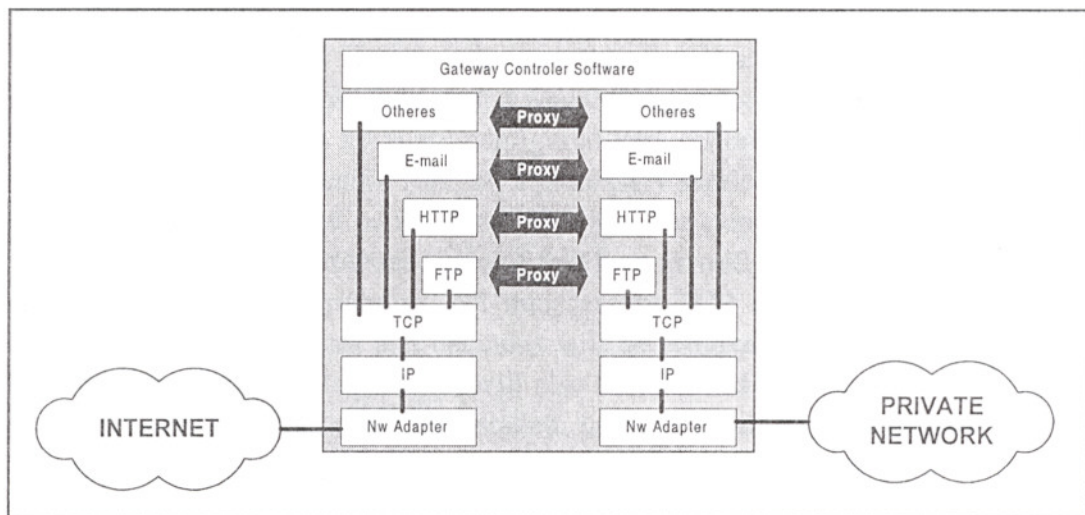
Proxy firewalls monitor traffic at the application level as shown in Figure 3.4. In the application proxy environment, a client application first connects to a process on the firewall machine that listens for client connections. After connecting to the proxy, the user is authenticated to the firewall. Next, the user indicates which server he or she needs to access. After receiving information about the requested server, the proxy connects to the desired remote host and relays the information being sent from the server to the client. At all times, the proxy application remains on the link and can limit, at the application level, what the client or server is doing. The advantage of proxy model is the lack of IP forwarding.

In essence, the client software views the proxy server as the actual server. Therefore, all traffic intended for the client goes to the proxy machine rather than to the actual server. By the same token, the actual server views the proxy server as the client; all traffic at the server appears to come from the proxy server. In this way, the proxy can

<sup>4</sup>Y. Rekhter, "Address Allocation for Private Internets", RFC 1918, p. 2

protect both the client and the server by authenticating the client, determining if the client can use the requested service, preventing attacks and prohibiting certain application-level events (such as FTP PUT or FTP GET). Proxy filters are less susceptible to attacks that hide data in legitimate traffic.

Application proxies can also verify that the interaction between client and server actually conforms to the protocol in use (i.e., HTTP or FTP). Therefore, proxy filters are more secure than packet filters.<sup>5</sup>



**Figure 3.4 Proxy Filter**

Proxy firewalls tend to have lower performance than packet filters, because they are more involved in the connection. Another disadvantage of this scheme is that a proxy application must be created for each networked service (one is used for FTP, another for Telnet, another for HTTP, and so forth) and proxy firewalls required modified user methods or specialized client applications to interact with the proxy.<sup>6</sup>

### 3.1.4 Hybrid Firewalls

Packet filters are fast and transparent to users, as opposed to the slower proxies that required custom client software. Proxy filters are more secure and flexible because the proxy could check the protocol and verify that every message corresponded to it, rather than simply allowing or denying packets based on their port numbers.

Hybrid firewalls can do what packet filters do and proxy filters do. The services best handled by packet filters (such as telnet) can be packet-filtered, while those best handled by proxies (such as FTP) can be proxied.<sup>7</sup> Current firewalls can do network-level encryption. Since firewalls control access to the network, they are an obvious point to place the encryption function.

<sup>5</sup> Anonymous, "Maximum Security", Macmillan Computer Publishing

<sup>6</sup> K. Maxon "Application Layer Firewalls vs. Network Layer Firewalls Which Is the Better Choice?", <http://www.seconf.net/info/fw/firewall.htm>

<sup>7</sup> E. Skoudis, "Fire in the Hole, E. Skoudis", <http://www.seconf.net/info/fw/fire.htm>

### 3.2 Firewall Architectures

Firewalls can be configured in a number of different architectures, provided various levels of security at different costs of installation and operation.

#### Definitions:

**De-Militarized Zone (Perimeter Network):** De-Militarized Zone (DMZ) is a network added between a protected network and an external network to provide an additional layer of security.

**Bastion Host:** Bastion Host is a host system that has been hardened to resist attack, and it installed on a network in such a way that it is expected to potentially come under attack. Effective bastion hosts are configured very differently from typical hosts. Each bastion host fulfills a specific role, all unnecessary services, protocols, programs, and network ports are disabled or removed. The specific steps to harden a particular bastion host depend upon the intended role of that host as well as the operating system and software that it will be running. All unnecessary TCP and UDP ports will be disabled; all non-critical services and daemons will be removed; as many utilities and system configuration tools as is practical will also be removed. All appropriate service packs, hot fixes, and patches should be installed. Logging of all security related events need to be enabled and steps need to be taken to ensure the integrity of the logs so that a successful intruder is unable to erase evidence of their visit.

#### 3.2.1 Screening Router (Packet Filter)

A screening router is a basic component of most firewalls. Typical screening routers have the ability to block traffic between networks or specific hosts, on an IP port level as shown in Figure 3.5. Some firewalls consist of nothing more than a screening router between a private network and the Internet. Screening routers carry disadvantages of packet filter firewalls.

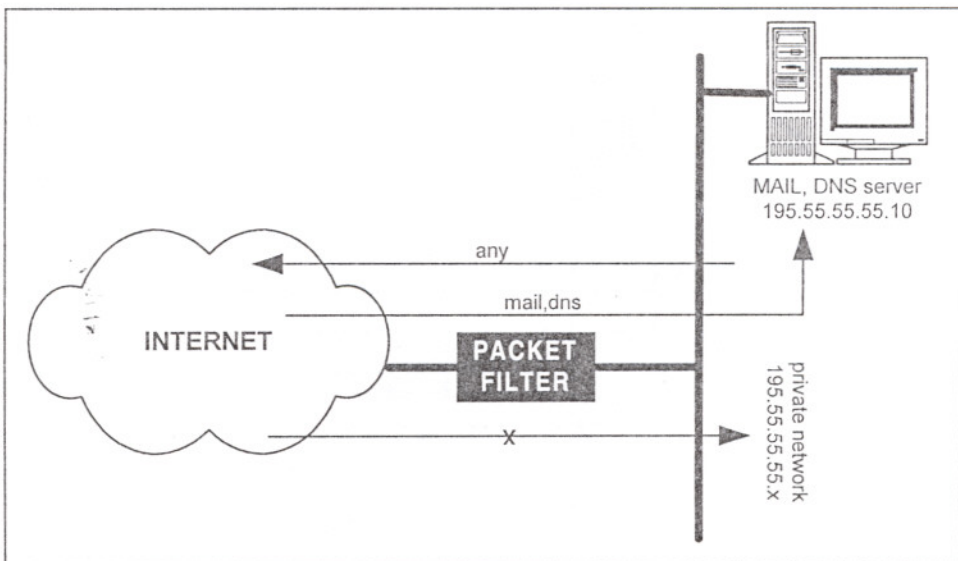


Figure 3.5. Packet Filter Firewall

### 3.2.2 Dual-Homed Host

The simplest firewall architecture utilizes a dual homed host. A dual-homed host is a computer that has separate network connections to two networks as shown in Figure 3.6. Any host could act as a router between the two networks, but this routing function is disabled when dual-homed hosts are used in firewall architectures. The host isolates the two networks from each other because the routing function is disabled. These systems cannot communicate with each other directly. A dual homed host can only provide services by proxying them. Dual homed host serve non-secure services such as WWW, DNS. Any one can access these services from outside.

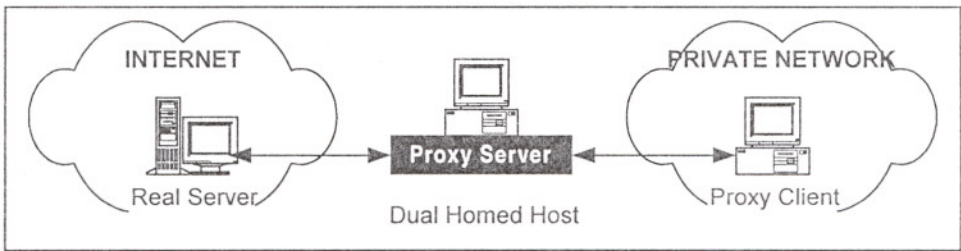


Figure 3.6. Dual Homed Host Firewall

The disadvantage of dual homed host is that managing this machine becomes very difficult and in case an intruder penetrates this machine it could take a lot of time to discover it.<sup>8</sup>

### 3.2.3 Screened Host

As shown in Figure 3.7, the primary security is provided by packet filtering and a bastion host sits on the internal network providing the required application. The screening router's packet filtering rules are configured such that the bastion host is the

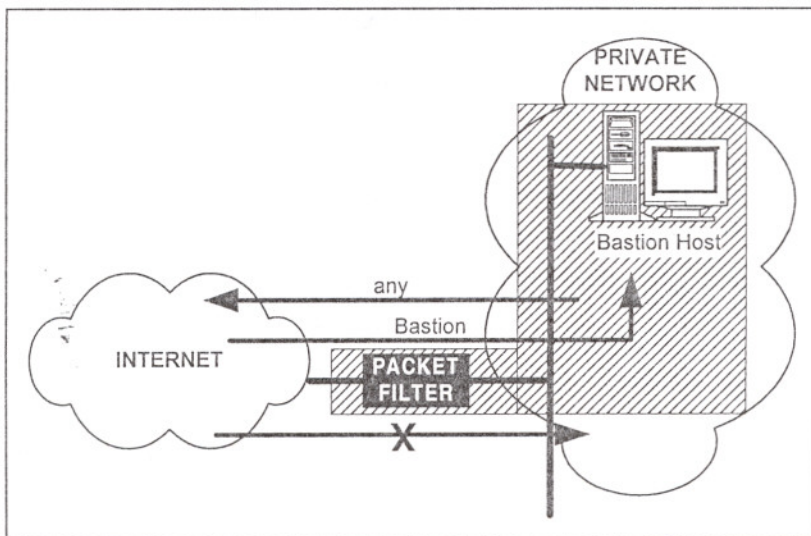


Figure 3.7 Screen Host Firewall

<sup>8</sup> IBM Corp. , "Internet Security in the Network Computing Framework", IBM Corp.

only host accessible from the Internet. Connections to the Internet may be routed through an application proxy on the bastion host, or in some cases, allowed directly through the screening router, depending on the network security policy.

The a screened host architecture adds an additional layer of security to the dual homed host architecture, as an intruder has to first bypass the screening router, and then the bastion host.<sup>9</sup> But this architecture allows packets to move from the Internet to the internal network. It may seem more risky than dual homed host architecture.

### 3.2.4 Screened Subnet

Screened subnet firewall architecture combines bastion hosts and packet filters as shown in Figure 3.8. In this case the subnetwork between the packet filters, which is also known as De-militarized Zone (DMZ), is used to put bastion host servers as a site for application services such as Web server. In this architecture, private network users can access Internet and bastion hosts. No one can access private network from Internet but anyone can access permitted bastion hosts from Internet.

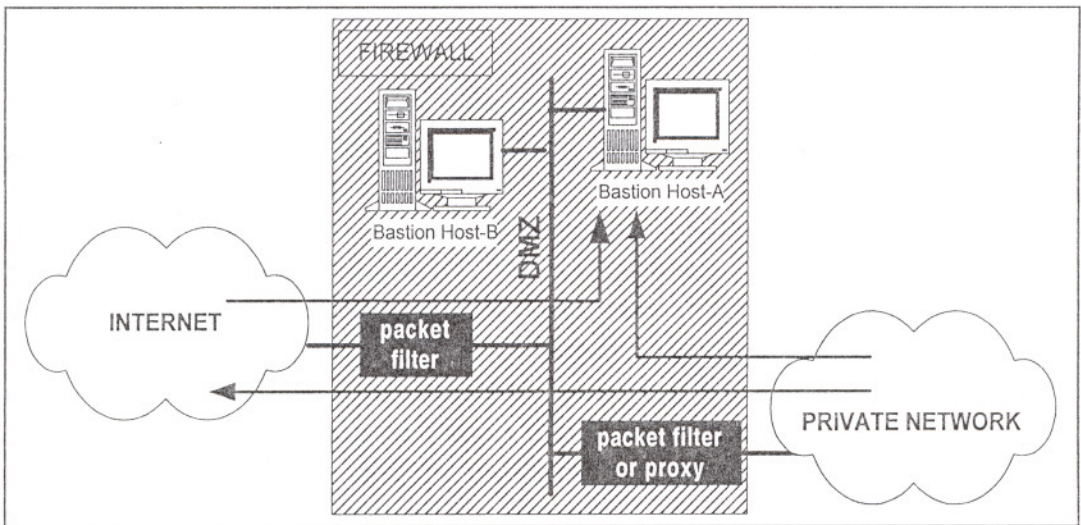


Figure 3.8 Screened Subnet Firewall

By their nature, bastion hosts are most vulnerable machines on network.<sup>10</sup> In screened subnet architecture, bastion hosts are protected by exterior packet filter. Another advantage from a security point of view is that this architecture can hide the internal network from the non-secure network, because each communication between the two networks needs to pass through the DMZ.<sup>11</sup>

<sup>9</sup> S. McGibbon, "Firewalls and Internet Security", <http://www.seconf.net/info/fw/steph>

<sup>10</sup> B. Chapman, "Building Internet Firewalls", O'Reilly, p. 128

<sup>11</sup> IBM Corp., "Internet Security in the Network Computing Framework", IBM Corp.

## Chapter 4

### THREATS FOR NETWORK SECURITY

Many of the global Internet's security vulnerabilities are inherent in the original protocol design. There are no security features built into IPv4 itself, and the few security features that do exist in other TCP/IP protocols are weak. This weakness causes many network security threats.

#### 4.1 Some Statistics About Security Incidents

Although it is not possible to have a 100% secure network, networks that are connected to the Internet are carrying great risks and people don't make enough effort to get precautions. Here are some statistics about security incidents:

42% of respondents acknowledged that they had experienced unauthorized use of computer. The distribution of these attacks is brute force password guessing (13.9% of attacks) and scanning (15% of attacks) to denial of service (16.2% of attacks) and data diddling (15.5% attacks).<sup>1</sup>

Another survey, which is done by CERT, shows that some software tools are used in 18.1% of all reported incidents. From these records, the largest category of tools was scripts or programs (15.4%). These consisted primarily of Trojan horses (10.5%) and sniffers (5.7%). The two general categories of toolkits were tools designed to exploit privileged or root access (1.2%), and scanners (2.6%). 45.3% of the reported incidents has specific vulnerabilities. The most frequently recorded vulnerability involved various problems with passwords (21.8%). Most of the password vulnerabilities were in three categories: password file copying (13.8%), password cracking (10.4%), and weak passwords (3.6%). The reputation of mail transfer agents for being "plagued with security problems" was confirmed in the CERT incident records, which contain numerous references to mail (18.5%). Problems with implementation of trusted hosts was recorded in a significant number of incidents (5.8%), as was configuration (5.7%), TFTP (5.5%), NIS (4.0%), FTP (4.0%), and NFS (3.2%).<sup>2</sup>

#### 4.2 Port Scanning

Port scanning is an attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service.<sup>3</sup> Port scanning is quite easy to detect, so intruders use a number of methods. For instance, many machines don't log connections until they're fully made, so an intruder can send an initial packet, with a SYN but no ACK, get back the response (another SYN if the port is open, a RST if it is not), and then stop there.

<sup>1</sup> R. Power, "Current and Future Danger", <http://www.gocsi.com/crreport.htm>

<sup>2</sup> J. Howard, "An Analysis Of Security Incidents On The Internet", <http://www.cert.org/research/JHThesis/Chapter16.html>

<sup>3</sup> R. Shirey, "Internet Security Glossary", RFC 2828, P.128



This is often called a SYNscan or a half-open scan. Although this won't get logged, it may have other unfortunate effects. If the scanner fails to send a RST when it stops (for instance, it may end up being a denial of service attack against the host or some intermediate device that's trying to keep track of open connections, like a firewall).

Intruders may also send other packets, counting a port as closed if they get a RST and open if they get no response, or any other error. Almost any combination of flags other than SYN by itself can be used for this purpose, although the most common options are FIN by itself, all options on, and all options off.

### 4.3 Packet Sniffers

A packet sniffer is a software application that uses a network adapter card to capture all network packets that are sent across a particular collision domain. Sniffers are used legitimately in networks today to aid in troubleshooting and traffic analysis. However, because several network applications send data in clear text (telnet, FTP, SMTP, POP3, and etc.), a packet sniffer can provide meaningful and often sensitive information, such as usernames and passwords.

Sniffing is a passive security attack in which a machine separate from the intended destination reads data on a network. Passive security attacks are those that do not alter the normal flow of data on a communication link or inject data into the link.<sup>4</sup>

Another problem with acquiring usernames and passwords is that users often reuse their login names and passwords across multiple applications and systems. In fact, many users employ a single password for access to all accounts and applications. If an application is run in client-server mode and authentication information is sent across the network in clear text, then it is likely that this same authentication information can be used to gain access to other corporate or external resources.

### 4.4 IP Spoofing

An IP spoofing attack occurs when an intruder inside or outside a network acts to be a trusted computer. The intruder either uses an IP address that is within the range of trusted IP addresses for a network or an authorized external IP address that is trusted and to which access is provided to specified resources on a network. IP spoofing attacks are often a launch point for other attacks. Intruder can do DoS attack which is using spoofed source addresses to hide his or her identity.

Normally, an IP spoofing attack is limited to the injection of malicious data or commands into an existing stream of data that is passed between a client and server application or a peer-to-peer network connection. To enable bi-directional communication, the intruder must change all routing tables to point to the spoofed IP address. An even simpler method for spoofing a client is to wait until the client system

---

<sup>4</sup>D. Atkins, P. Buis, "Internet Security Professional Reference", New Riders

is turned off and then impersonate the client's system.<sup>5</sup> Another approach intruders sometimes take is to simply not worry about receiving any response from the applications. If an intruder tries to obtain a sensitive file from a system, application responses are unimportant. If an intruder manages to change the routing tables to point to the spoofed IP address, the intruder can receive all the network packets that are addressed to the spoofed address and reply just as any trusted user can.

## 4.5 Denial of Service

Denial of service (DoS) attacks are also among the most difficult to completely eliminate. DoS attacks are different from most other attacks because they are generally not targeted at gaining access to private network or the information on private network. These attacks focus on making a service unavailable for normal use, which is typically accomplished by exhausting some resource limitation on the network or within an operating system or application. The crudest and easiest form to try to fill up someone's disk, by mailing or using FTP to send a few hundred megabytes.<sup>6</sup>

When involving specific network server applications, such as a Web server or an FTP server, these attacks can focus on acquiring and keeping open all the available connections supported by that server, effectively locking out valid users of the server or service. DoS attacks can also be implemented using common Internet protocols, such as TCP and Internet Control Message Protocol (ICMP). Most DoS attacks exploit a weakness in the overall architecture of the system being attacked rather than a software bug or security hole.

There are many kind of DoS attacks. These attacks include the followings:

### 4.5.1 TCP SYN Flood

When a client attempts to establish a TCP connection to a server, the client and server exchange a set sequence of messages. This connection technique applies to all TCP connections--telnet, Web, email, etc. The client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending SYN-ACK message to the client. The client then finishes establishing the connection by responding with an ACK message. The connection between the client and the server is then open, and the service-specific data can be exchanged between the client and the server.

The potential for misuse arises at the point where the server system has sent an acknowledgment (SYN-ACK) back to client but has not yet received the ACK message. This is half-open connection. The server has built in its system memory a data structure describing all wanted connections. This data structure has limited size, and it can be made to overflow by intentionally creating too many half-open connections. In most cases, the victim of such an attack will have difficulty in accepting any new incoming

---

<sup>5</sup> J. Wack, "Keeping Your Site Comfortably Secure: An Introduction to the Internet and Internet Security", NITS Special Publications, 800-10

<sup>6</sup> W. Cheswick, S. Bellovin, "Firewalls and Internet Security", Addison-Wesley, p. 165

network connection. At the end, the system may exhaust memory, crash, or be rendered otherwise inoperative.

Creating half-open connections is easily accomplished with IP spoofing. The attacking system sends SYN messages to the server; these appear to be legitimate but in fact reference a client that is unable to respond to the SYN-ACK messages. This means that the final ACK message will never be sent to the server.

#### **4.5.2 Ping of Death**

The TCP/IP specification allows for a maximum packet size of up to 65536 bytes, containing a minimum of 20 bytes of IP header information and zero or more bytes of optional information, with the rest of the packet being data. It is known that some systems will react in an unpredictable fashion when receiving oversized IP packets. This causes crashing, and rebooting.

Internet Control Message Protocol (ICMP) packets issued via the "ping" command have been used to trigger this behavior. ICMP is a subset of the TCP/IP suite of protocols that transmits error and control messages between systems. Two specific instances of the ICMP are the ICMP ECHO\_REQUEST and ICMP ECHO\_RESPONSE datagrams. These two instances can be used by a local host to determine whether a remote system is reachable via the network; this is commonly achieved using the "ping" command.

#### **4.5.3 Smurf Attack**

Smurf is a DoS attack technique that takes advantage of the ICMP. Smurf is installed on a computer using a stolen account, and then continuously "pings" one or more networks of computers using a forged source address. This causes all the computers to respond to a different computer than actually sent the packet.

#### **4.5.4 UDP Port Denial-of-Service Attack**

When a connection is established between two computers by UDP service, each of which produces output, these two services can produce a very high number of packets that can lead to a denial of service on the machines where the services are offered. Anyone with network connectivity can launch an attack; no account access is needed.

#### **4.5.5 Email Bombing and Spamming**

Email bombing/spamming is characterized repeatedly sending an identical email message to hundreds or thousands of users. It refers to sending email. Email spamming can be made worse if recipients reply to the email. It may also occur innocently. Email bombing/spamming may be combined with email "spoofing", making it more difficult to determine whom the email is actually coming from.

## 4.6 Password Attacks

Intruders can implement password attacks using several different methods, including brute-force attacks, Trojan horse programs, IP spoofing, and packet sniffers. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account and/or password. These repeated attempts are called brute-force attacks. Often, a brute-force attack is performed using a program that runs across the network and attempts to log in to a shared resource, such as a server.

## 4.7 Man in the Middle Attacks

A man-in-the-middle attack requires that the intruder have access to network packets that come across a network. An example of such a configuration could be someone who has access to all network packets transferred between two networks. Such attacks are often implemented using network packet sniffers and routing and transport protocols. The possible uses of such attacks are theft of information, hijacking of an ongoing session to gain access to private network resources, traffic analysis to derive information about a network and its users, denial of service, corruption of transmitted data, and introduction of new information into network sessions. These attacks tend to be problems only if one of the involving sites has hostile users who have physical access to the network.<sup>7</sup>

## 4.8 Hijacking

Hijacking attacks allow an intruder to take over an open terminal or login session from a user who has been authenticated and authorized by the system. Hijacking attacks generally take place on a remote computer, although it is sometimes possible to hijack a connection from a computer on the route between the remote computer and local computer. Hijacking a connection involves predicting the next packet in a TCP communications session between two other parties and replacing it with internal network packet. For example, hijacking could be used by an intruder to insert a command into a Telnet session. To hijack successfully, an intruder must either make an educated guess about the TCP sequence information, or be able to sniff the packet. Hijacking is a threat because the intruder can wait for users to authenticate themselves, and then the intruder can take over the authenticated connection. Hijacking of a connection can happen no matter how strong the authentication required to start the connection.

## 4.9 Predicting TCP Initial sequence numbers

The sequence number is used to acknowledge receipt of data. At the beginning of a TCP connection, the client sends a TCP packet with an initial sequence number, but no acknowledgment. If there is a server application running at the other end of the connection, the server sends back a TCP packet with its own initial sequence number,

---

<sup>7</sup> B. Chapman, "Building Internet Firewalls", O'Reilly, p. 185

and an acknowledgment: the initial sequence number from the client's packet plus one. When the client system receives this packet, it must send back its own acknowledgment: the server's initial sequence number plus one. And TCP connection continues.

Theoretically, it can't be spoof any protocol based upon TCP connections. This is because both sides of a TCP connection choose their own Initial Sequence Number. In theory, this is a completely random number that cannot be guessed. In some weak TCP/IP implementations, it can sometimes be easily guessed.

When the intruder has the initial sequence number of the connection, the next and final step is to estimate how much TCP/IP data has been sent to the receiver. This estimate added to the initial sequence number estimates the current sequence number.

#### **4.10 Replay Attack**

An intruder who can't take over a connection or change a connection may still be able to do damage simply by saving up information that has gone past and sending it again. We've already discussed one variation of this attack, involving passwords.

There are two kinds of replays, one has certain pieces of information (for instance, the password attacks), and the other simply resends the entire packet which is sent before from internal. If encryption is made in session, it's possible to reuse a packet without knowing what's in it.

#### **4.11 Application Layer Attacks**

Application layer attacks can be implemented using several different methods. One of the most common methods is exploiting well-known weaknesses in software that are commonly found on servers, such as sendmail, HTTP, and FTP. By exploiting these weaknesses, intruders can gain access to a computer with the permissions of the account running the application, which is usually a privileged system-level account. These application layer attacks are often widely publicized in an effort to allow administrators to rectify the problem with a patch.

The primary problem with application-layer attacks is that they often use ports that are allowed through a firewall. For example, an intruder executing a known vulnerability against a Web server often uses TCP port 80 in the attack. Because the Web server serves pages to users, a firewall needs to allow access on that port. From a firewall's perspective, it is merely standard port 80 traffic.

#### **4.12 Network Scanners**

Network Scanners refers to the overall act of learning information about a target network by using publicly available information and applications. When intruders attempt to penetrate a particular network, they often need to learn as much information as possible about the network before launching attacks. This can take the form of DNS

queries, ping sweeps, and port scans. DNS queries can get such information as who owns a particular domain and what addresses have been assigned to that domain. Ping sweeps of the addresses revealed by the DNS queries can present a picture of the active host. After such a list is generated, port-scanning tools can cycle through all well-known ports to provide a complete list of all services running on the hosts discovered by the ping sweep. At the end, the intruder can examine the characteristics of the applications are running on the hosts. This information can be used attack later.

#### **4.13 DNS Security Problems**

Domain Name System (DNS) is the way that Internet domain names are located and translated into Internet Protocol (IP) addresses. Because maintaining a central list of domain name/IP address correspondences would be impractical, the lists of domain names and IP addresses are distributed throughout the Internet in a hierarchy of authority. When a DNS machine is compromised, this machine has been a victim of a spoofing. All private connections of the Secret Services were re-routed to an intruder's home server.

#### **4.14 Trust Exploitation**

Trust exploitation refers to an attack where an individual takes advantage of a trust relationship within a network. DNS, SMTP, and HTTP servers are places in the same network segments, so that compromise of one system can lead to the compromise of other systems. Because they might trust other systems attached to their same network. Another example is a system on the outside of a firewall that has a trust relationship with a system on the inside of a firewall. When the outside system is compromised, it can leverage that trust relationship to attack the inside network.

#### **4.14 Port Redirection**

Port Redirection attacks are a type of trust exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped. The host on the outside can reach the host on the public services segment, but not the host on the inside. The host on the public services segment can reach the host on both the outside and the inside. If intruders were able to compromise the public services segment host, they could install software to redirect traffic from the outside host directly to the inside host. Though neither communication violates the rules implemented in the firewall, the outside host has now achieved connectivity to the inside host through the port redirection process on the public services host.

#### **4.15 Unauthorized Access**

While not a specific type of attack, unauthorized access attacks refer to the majority of attacks executed in networks today. In order for someone to brute-force a telnet login, they must first get the telnet prompt on a system. Upon connection to the telnet port, a message might indicate: "authorization required to use this resource." If

the intruder continues to attempt access, his actions become "unauthorized". These kinds of attacks can be initiated both on the outside and inside of a network.

#### **4.16 Virus and Trojan Horse Applications**

The primary vulnerabilities for end-user workstations are viruses and Trojan horse attacks. Viruses refer to malicious software that is attached to another program to execute a particular unwanted function on a user's workstation.

Attachments, or HTML files may contain malicious code in the form of CGI script, Java, JavaScript, VBScript, or ActiveX controls. A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool. An example of a Trojan horse is a software application that runs a simple game on the user's workstation. While the user is occupied with the game, the Trojan horse mails a copy of itself to every user in the user's address book. Then other users get the game and play it, thus spreading the Trojan horse.

#### **4.17 Remote Procedure Call (RPC)**

RPC is generally used in SUN system. The problem is that a number of RPC services are very difficult to filter effectively because the associated servers listen at ports that are assigned randomly at system startup. A service known as portmapper maps initial calls to RPC services to the assigned service numbers, but there is no such equivalent for a packet filtering router. Since the router cannot be told which ports the services reside at, it isn't possible to block completely these services unless one blocks all UDP packets (RPC services mostly use UDP). Blocking all UDP would be problems for it also blocks potentially necessary services such as DNS.

#### **4.18 Insiders**

71% of incidents which is reported are insider attacks<sup>8</sup>. Insiders may do attacks intentionally or accidentally. One study estimates that 55 % of all security incidents actually result from naive or untrained users doing things they shouldn't.<sup>9</sup> Denial of service incidents, for example, running an executable file, which is, attached an email may cause sending this file to all mail addresses. If insecure modems are located in local network department behind the firewall, this is a potential hole.

---

<sup>8</sup> R. Pethia, "Internet Security Trends", <http://www.cert.org/present/internet-security-trends/tsld008.htm>

<sup>9</sup> R. Power, "Current and Future Danger", <http://www.gocsi.com/crreport.htm>

## Chapter 5

### COUNTERMEASURES AGAINST THREATS

In previous chapter, possible threats are described. Security measures are needed to reduce risks against these threats. This chapter aims to describe how prevention methods can be used for each defined threat, and afterwards a decision will be derived from the prevention method. Later, these decisions will be used for building rule set of firewall.

#### 5.1 Port Scanning

Packet filter Firewalls are good defense against port scanners. They have to block unassigned port traffic (traffic to ports with unassigned services).

DECISION: Block unassigned port traffics.

#### 5.2 Packet Sniffers

The threat of packet sniffers can be minimized in several ways:

Using strong authentication is a first option for defense against packet sniffers. Strong authentication (like one-time-passwords) can be broadly defined as a method of authenticating users that cannot easily be exploit.

DECISION: Use strong authentication mechanism.

Another method to counter the use of packet sniffers in private environment is to deploy a switched infrastructure. For example if an entire university deploys switched Ethernet, intruders can only gain access to the traffic that flows on the specific port to which they connect. A switched infrastructure obviously does not eliminate the threat of packet sniffers, but it can greatly reduce their effectiveness.

DECISION: Use switched infrastructure if possible.

The most effective method for countering packet sniffers does not prevent or detect packet sniffers, but rather renders them irrelevant. If a communication channel is cryptographically secure, the only data a packet sniffer will detect is cipher text (a seemingly random string of bits) and not the original message.

DECISION: Use cryptographically secure channel.

#### 5.3 IP Spoofing

The threat of IP spoofing can be reduced, but not eliminated. The most common method for preventing IP spoofing is to properly configure access control. To reduce the effectiveness of IP spoofing, access control configuration must be done to deny any traffic from the external network that has a source address that should reside on the



internal network. Note that this only helps prevent spoofing attacks if the internal addresses are the only trusted addresses. If some external addresses are trusted, this method is not effective.

DECISION: If the source address of the incoming packet is an address which is belongs to the internal address, block this datagram.

Network users can also be prevented from spoofing other networks by preventing any outbound traffic on private network that does not have a source address in organization's own IP range. The belonged ISP can also implement this type of filtering, which is referred in RFC 2827 filtering. This filtering denies any traffic that does not have the source address that was expected on a particular interface as shown in Figure 5.1.

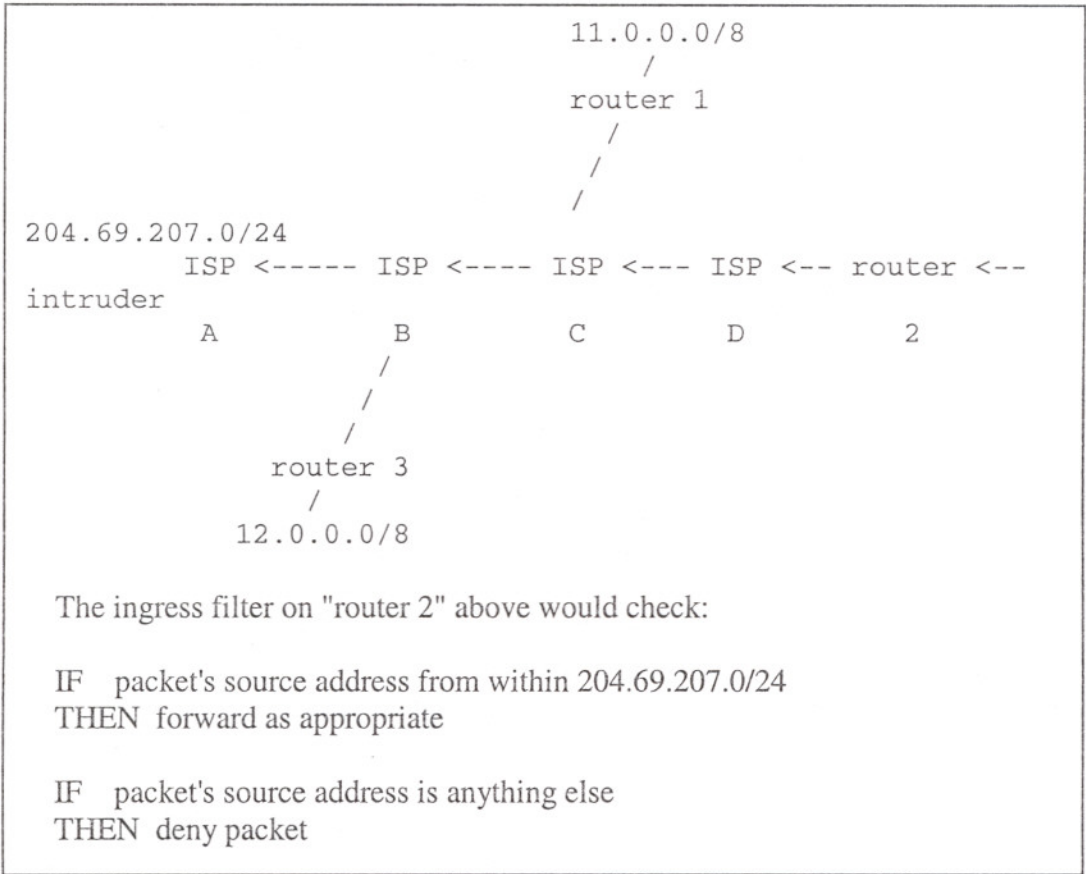


Figure 5.1 RFC 2827 filtering<sup>1</sup>.

DECISION: Advice ISP to use RFC 2827 filtering.

DECISION: Use Network Address Translation (NAT) and NAT reserved IP addresses for internal network.

DECISION: Don't let IP addresses which are reserved for NAT go out and in.

<sup>1</sup>P. Ferguson, D. Senie, "Network Ingress Filtering", RFC 2827, p. 4

The most effective method for decreasing the threat of IP spoofing is the same as the most effective method for decreasing the threat of packet sniffers: namely eliminating its effectiveness. IP spoofing can function correctly only when devices use IP address-based authentication. Therefore, if additional authentication methods are used, IP spoofing attacks are irrelevant. Cryptographic authentication is the best form of additional authentication, but when that is not possible, strong two-factor authentication using One Time Password (OTP) can also be effective.

DECISION: Use cryptographic authentication.

## 5.4 Denial of Service

Denial of service (DoS) attacks are also among the most difficult to completely eliminate. Aggressive filtering can do a lot to protect private network; but there are no absolute guarantees; it can be very hard to tell difference between genuine messages, ordinary failures, and enemy actions.<sup>2</sup>

### 5.4.1 TCP SYN Flood

With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, it is possible to reduce the number of IP-spoofed packets entering in and exiting out from private network.

Currently, the best method is to install a firewall that restricts the input to the external interface of network by not allowing a packet through if it has a source address from internal network. In addition, outgoing packets that have a source address different from the internal network cause IP spoofing attack from originating from internal network. These packets should be filtered to prevent a source IP spoofing attack

The combination of these two filters would prevent outside intruders from sending internal network packets pretending to be from internal network. It would also prevent packets originating within internal network from pretending to be from outside internal network.

DECISION: Check source address for going out packets source addresses and block packets which don't belong to internal network.

The long-term solution to this is that adapting TCP algorithms in the kernel to recognize attacks, possible reduce timeouts based on network speed etc. Many newer firewalls provide protection against SYN flooding.<sup>3</sup>

DECISION: Use SYN flood resistant firewall.

---

<sup>2</sup> W. Cheswick, S. Bellovin, "Firewalls and Internet Security", Addison-Wesley, p. 166

<sup>3</sup> S. Boran, "IT Security Cookbook", [http://secinf.net/info/misc/boran/Firewalls\\_Securing\\_externalNetwork\\_connections.htm](http://secinf.net/info/misc/boran/Firewalls_Securing_externalNetwork_connections.htm)

### 5.4.2 Ping of Death

The best way to prevent Ping of Death is to patch operating system to a version that is not susceptible. The kernel will no longer attempt to reassemble packets that exceed the maximum length.

DECISION: Use OS patch which is strong to the ping of death.

There is an effectively way to block the attack at firewall level. Firewall assembles every fragmented IP packet and check if it's too long before passing the fragments on to the destination machine. But his can be time and CPU consuming.<sup>4</sup>

The other solution to block ping of death is to drop fragmented packets. Because fragmentation is almost never needed. Most communication runs over TCP, which does its own segmentation which is more efficient. Therefore, if thee are any fragmentation on internal network, it should be examined closely to see if it indicates an attack.<sup>5</sup>

A common question is which ICMP traffic should be filtered by a firewall. ICMP consists of control messages, some of which are needed, others are desirable, and still others can be used to cause problems on internal network.

DECISION: Block fragmented packets.

### 5.4.3 Smurf Attack

One solution to prevent network from being used as an intermediary in this attack is to disable IP-directed broadcasts at router. In almost all cases, IP-directed broadcast functionality is not needed.

Network service providers and corporate network operators are urged to ensure their networks are not susceptible to directed broadcast packets originating outside their networks.<sup>6</sup>

DECISION: Block IP-broadcast packets.

### 5.4.4 UDP Port Denial-of-Service Attack

This attack is most readily exploited using the echo services. It isn't necessary for outside traffic. To protect against similar attacks against other services, disabling all unused UDP services on hosts and blocking at firewalls all UDP ports less than 900 with the exception of specific services that is required, such as DNS.

DECISION: Disable echo services on the host and filter them at the firewall or Internet gateway.

---

<sup>4</sup> W. Sonnenreich, T. Yates, "Building Linux and OpenBSD Firewalls", Wiley, p. 26

<sup>5</sup> R. Graham, "Hacking Lexicon", <http://www.robertgraham.com/pubs/hacking-dict.html>

<sup>6</sup> D. Senie, "Changing the Default for Directed Broadcasts in Routers", RFC 1812, p. 2

### 5.4.5 Email Bombing and Spamming

There is no way to prevent email bombing or spamming<sup>7</sup> (other than disconnecting from the Internet), and it is impossible to predict the origin of the next attack. It is trivial to obtain access to large mailing lists or information resources that contain large volumes of email addresses that will provide destination email addresses for the spam. After monitoring the source of the email bomb/spam, it can be configured firewall to prevent incoming packets from that address.

DECISION: Use Intruder Detection System.

### 5.5 Password Attacks

Password attacks can be easily eliminated by not relying on plain-text passwords in the first place. Using One Time Password and/or cryptographic authentication can virtually eliminate the threat of password attacks. Unfortunately, not all applications, hosts, and devices support these authentication methods. When standard passwords are used, it is important to choose a password that is difficult to guess. The best passwords are randomly generated but are very difficult to remember, often leading users to writing write their passwords down.

DECISION: Use One Time Password and/or cryptographic authentication.

### 5.6 Man-in-the-Middle Attacks

Man-in-the-middle attacks can be effectively reduced only through the use of cryptography. If someone hijacks data in the middle of a cryptographically private session, all the intruder will see is cipher text and not the original message. Note that if an intruder can learn information about the cryptographic session (such as the session key) man-in-the-middle attacks are still possible.

DECISION: Use cryptographic session.

### 5.7 Hijacking

Hijacking by intermediate sites can be avoided using end-to-end integrity protection. If end-to-end integrity protection is used, intermediate sites will not be able to insert authentic packets into the data stream (because they don't know the appropriate key and the packets will be rejected) and therefore won't be able to hijack sessions traversing them.

DECISION: Use end-to-end integrity protection

---

<sup>7</sup> M. Goncalves, "Firewalls Complete", McGraw-Hill Companies

## 5.8 Predicting TCP Initial sequence numbers

The only way to deal with this threat completely with current standardized technology is to use a combination approach. Initial sequence numbers must be unpredictable and fall throughout the full range of four billion. TCP/IP data must be encrypted so that unencrypted or mis-encrypted data will not be confused with valid commands. It is possible that an intruder may cause a TCP/IP connection to reset because of garbage injected into a connection by an intruder with a sniffer.

DECISION: Use OS patch against predictable TCP Initial Sequence numbers.

DECISION: Encrypt TCP/IP data.

## 5.9 Replay Attack

Replaying packets doesn't work with TCP because of the sequence numbers, but there's no reason for it to fail with UDP-based protocols. The only protection against it is to have a protocol that will reject the replayed packet (for instance, by using timestamps or embedded sequence numbers of some sort). The protocol must also do some sort of message integrity checking to prevent an intruder from updating the intercepted packet.

Methods which prevent replay attacks in authentication are known as strong authentication and can be divided into three classes: shared sequence, challenge/response and asymmetric key.<sup>8</sup>

DECISION: Use OS patch against predictable TCP Initial Sequence numbers.

DECISION: Encrypt TCP/IP data.

## 5.10 Application Layer Attacks

Application layer attacks can never be completely eliminated. New vulnerabilities are always being discovered and publicized to the Internet community. The best way to reduce the risk is by practicing good system administration. Applying latest patches and analyzing logs can reduced risks. In addition, using Intrusion Detection Systems (IDSs) can aid in this effort. There are two complementary IDS technologies:

IDS operates by watching all packets traversing a particular collision domain. When IDS sees a packet or series of packets that match a known or suspect attack, it can flag an alarm and/or terminate the session.

IDS operates by using attack signatures. Attack signatures are the profile for a particular attack or kind of attack. They specify certain conditions that must be met before traffic is deemed to be an attack. In the physical world, IDS can be most closely

---

<sup>8</sup> A. Cormack, "Web Security ", <http://www.jisc.ac.uk/acn/authent/cormack.html>

compared to an alarm system or security camera. IDS system's greatest limitation is the amount of false-positive alarms a particular system generates. Tuning IDS to prevent such false alarms is critical to the proper operation of IDS in a network.

DECISION: Use Intrusion Detection System.

### **5.11 Network Scanners**

Network scan cannot be prevented entirely. If ICMP echo and echo-reply is turned off on edge routers, for example, ping sweeps can be stopped, but at the expense of network diagnostic data. However, port scans can easily be run without full ping sweeps; they simply take longer because they need to scan IP addresses that might not be live. IDS at the network and host levels can usually notify an administrator when a network scanning attack is underway. This allows the administrator to better prepare for the coming attack or to notify the ISP who is hosting the system that is launching the scan probe.

DECISION: Use Intrusion Detection System.

### **5.12 DNS Security Problems**

A DNS spoofing is not an easy task. It's not enough for an intruder to gain access to the DNS server.

DECISION: Use Intrusion Detection System.

### **5.13 Trust Exploitation**

Trust exploitation-based attacks can be minimized through tight constraints on trust levels within a network. Systems on the outside of a firewall should never be absolutely trusted by systems on the inside of a firewall. Such trust should be limited to specific protocols and should be authenticated by something other than an IP address where possible.

DECISION: Use privacy and authentication mechanism.

### **5.14 Port Redirection**

Port redirection can primarily be lessened through the use of proper trust models. Assuming a system under attack, host-based IDS can help detect and prevent an intruder installing such utilities on a host.

DECISION: Use Intrusion Detection System.

DECISION: Block unnecessary ports.

## 5.15 Unauthorized Access

It is very simple to decrease unauthorized access attacks. They involve reducing or eliminating the ability of an intruder to gain access to a system using an unauthorized protocol. An example would be preventing intruders from having access to the telnet port on a server that needs to provide Web services to the outside. If an intruder cannot reach that port, it is very difficult to attack it. The primary function of a firewall in a network is to prevent simple unauthorized access attacks.

DECISION: Use privacy and authentication mechanism.

DECISION: Don't manage servers remotely without SSH.

## 5.16 Virus and Trojan Horse Applications

These kinds of applications can be contained through the effective use of anti-virus software at the user level and potentially at the network level. Anti-virus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network. Keeping up-to-date with the latest developments in these sorts of attacks can also lead to a more effective posture against these attacks. As new virus or Trojan applications are released, enterprises need to keep up-to-date with the latest anti-virus software, and application versions. And clients shouldn't open any file unless they know exactly where it came from, or you know exactly what the program that opens it can do.

DECISION: Use updated anti-virus software.

DECISION: It is necessary to call attention to the users these risks.

## 5.17 RPC

The problem is that a number of RPC (Remote Procedure Call) services are very difficult to filter effectively because the associated servers listen at ports that are assigned randomly at system startup.

DECISION: Block all unnecessary UDP ports.

DECISION: If it isn't necessary, don't use RPC service.

## 5.18 Insiders

Insider attacks threaten four sectors. These are outside of the internal network, bastion hosts where is settled in DMZ, internal servers and other inside users. Building DMZ and firewalls in DMZ minimize the insider attacks which aim foreign servers and bastion hosts in DMZ. But these countermeasures don't protect internal servers and other workstations of inside users. Putting a firewall in front of all internal workstations is not a practical and economical way to mitigate internal attacks. Internal networks have an advantage not to depend on outside network. It is possible to build

authenticated and encrypted LAN infrastructure for internal network. Thus weakness of TCP/IPv4 may be mitigated by using IPsec, etc. Proposing any authentication and encryption method is beyond of this thesis.

DECISION: Authenticated and encrypted LAN infrastructure should be built.

The other insider threat is that insider user may connect a dial-up modem near his workstation and he may access his computer from outside by public telephone network. Modem backdoor may be used by intruder. Building firewalls can't recognize this weakest link.

DECISION: It is necessary to inform users about network security and security personnel have to check the physical network infrastructure against modem backdoor.

İZMİR YÜKSEK TEKNOLOJİ ENSTİTÜSÜ  
REKTÖRLÜĞÜ  
Kütüphane ve Dokümantasyon Daire Başkanı



## Chapter 6

### ASSETS AND NEEDS OF ACADEMIC ENVIRONMENT NETWORK

All organizations have their objects while they are accomplishing their functions. These objects turn to assets and needs when organization cannot survive their mission without these objects. Publishing information, researching in Internet, high availability, data privacy and serving administrative and academic information via database and application software are the assets and needs of an academic environment. In this chapter, assets and needs are evaluated and then a decision is made after evaluation. If the evaluated asset is not very necessary for academic environment and threat against this asset cannot be stopped, then decision will be not to use this asset. If the evaluated asset is very necessary, then the decision will be to define the threats and to prevent the asset against attacks by a security tool.

#### 6.1 Electronic Mail

The use of Internet email to carry critical communications is growing exponentially. While email provides a low cost means of communicating with academic environment there are a number of security issues related to the use of electronic mail. Internet email addresses are easily spoofed and sniffed. Standard SMTP mail provides no integrity checking. Also, an email server requires access to the outside world; most email servers accept input from any source. Email servers are target of DoS.

DECISION: Email service is needed by academicians and they need to access their mail system remotely in a secure way.

DECISION: Email servers are target of DoS.

#### 6.2 Network News Transfer Protocol (NNTP)

NNTP is used to transfer news across the Internet. NNTP penetrates any way to the internal network. NNTP isn't like mail, anyone wants to get and send mail, so it's not particularly difficult to secure. The biggest security issue with news is what to do with private news groups.

DECISION: Private news groups and public news groups should be separated each other. Each one should have their own servers.

#### 6.3 Real Time Conferencing Services

Talk, IRC, AOL, and ICQ are real time conferencing services. In addition to them, there are Web based services. Web based services have fewer vulnerabilities. All of them need a client software. Real time conferencing services don't support security.

DECISION: Real Time Conferencing Services have no security.

## 6.4 World Wide Web (WWW)

The Internet greatly simplifies the task of providing information to students, teachers, and citizens. The Web is growing in popularity exponentially because of its ease of use and the powerful ability to concentrate information services. If a Web server is available to the Internet community, it is especially important that confidential information not be co-located on the same host as that server. Web servers are target of DoS.

DECISION: Academicians and other people want to use WWW service and academicians also want to update their web pages.

DECISION: WWW servers are target of DoS.

## 6.5 File Transfer (FTP, TFTP)

FTP and TFTP both allow users to receive and send electronic files in a point-to-point manner. FTP requires authentication. TFTP is designed to be implemented in ROM for booting diskless systems and TFTP doesn't require authentication. For this reason, TFTP should not be permitted as much as possible. Improperly configured FTP servers can allow intruders to copy, replace and delete files at will, anywhere on a host, so it is very important to configure this service correctly. FTP and TFTP servers are target of DoS.

DECISION: Academicians and other people want to use FTP service and academicians also want to update their files.

DECISION: FTP and TFTP servers is target of DoS.

DECISION: TFTP server shouldn't open to the public.

## 6.6 NFS

The Network File Service allows hosts to share common disks. NFS is frequently used by diskless hosts who depend on a disk server for all of their storage needs. Today it isn't widely used in academic environments. NFS has no built-in security.

DECISION: NFS service shouldn't open to the public.

## 6.7 Domain Name Servers

The Internet and local network use the Domain Name System (DNS) to perform address resolution for host and network names. The Name-to-address resolution is critical to the secure operation of any network. An intruder who can successfully control or impersonate a DNS server can re-route traffic to subvert security protections.

DECISION: DNS servers should be placed in a controlled area. They should be open for public and local users.

DECISION: DNS servers are target of DoS.

## 6.8 Password and Key Servers

Password and key servers generally protect their vital information with encryption algorithms. However, even a one-way encrypted password can be determined by a dictionary attack. It is therefore necessary to ensure that these servers are not accessible by hosts which do not plan to use them for the service, and even those hosts should only be able to access the service.

DECISION: Password and key servers should be placed in a controlled area. They should be open for remote and local trusted users.

DECISION: Password and key servers are target of DoS.

## 6.9 Routers

Routers control access from every network to every network. They advertise networks and filter who use them, and they are potentially an intruder's best friends. Router security is a critical element in any security deployment. By their nature, routers provide access and, therefore, they should be secure to reduce the likelihood that they are directly compromised.

DECISION: Routers are target of IPspoofing and DoS.

DECISION: Routers should have robust software.

## 6.10 Firewalls and Intrusion Detection Systems (IDS)

A firewall and IDS provides a number of security enhancements. It allows sites to concentrate services through a specific host to allow monitoring, hiding of internal structure, etc. This funneling of services creates an attractive target for a potential intruder.

DECISION: Firewalls and IDS are target of DoS.

## 6.11 Remote access

Telnet, rlogin, X-window commands provide a means for remotely logging in to computers over network connections. Many personal computers come equipped with TCP/IP software that also provides telnet capability. Telnet usually requires a username/password pair be sent over the network connection in the clear. This is a major security weakness.

DECISION: Remote access via Telnet is necessary in a secure way.

## 5.12 Information Transactions

Providing information is a major element of computing. Such information may take a variety of forms such as dynamic data, static data, historic information, graph, etc. These data may be store in a database and changed by an application program. Using the Internet to provide these services is substantially less expensive and flexible. Confidentiality, integrity and availability of the information provided are key security concerns that require security controls and policy.

The biggest security issue with information transaction is what to do internal administrative information transactions.

DECISION: Private information transactions and public information transactions should be separated from each other. They should have their own servers.

DECISION: Administrative information is vulnerable so it should be placed in private network No one can access this information remotely.

DECISION: Less sensitive information may be placed out of internal network.

## 6.13 High Availability

As use of the Internet becomes more critical to routine operations, security controls protecting Internet connections often need to support requirements for high availability or non-stop operations. These requirements often have a major impact on security policy, requiring decisions between the cost of redundant configurations versus the cost of temporarily operating without security controls.

DECISION: An appropriate balance is needed between high aviability and security control.

## 6.14 Ease of Use

The user population of many systems connected to the network may range from secretaries to academic staff, from students to their families. A frequent requirement is often that all applications are easy to use by the typical user population. This is not an easy requirement to quantify, but from a security perspective it can be often get translated as: "If security controls get in the way of people doing their jobs, a way will be figured out to bypass the security controls."

Two key elements of ease of use are reducing the number of times a user has to authenticate to the system and designing on interface for security controls to match the requirements or preferences of the user population.<sup>1</sup>

DECISION: The combination of approaches shows that an appropriate balance is needed between security and easy of use for academic environment.

---

<sup>1</sup> D Safford, "How to pick an Internet Firewall", Texas A&M University, USENIX Security Symposium

## 6.15 Openness

Academic organizations don't normally restrict access into or out of their network. This reflects the traditional openness of the academic environment. Academic organizations such as universities typically have the most trouble setting up a firewall. This is due to notions of academic freedom. Firewalls seem against academic freedom and openness, but all of the network security attacks also threaten high availability, ease usage and privacy of computer network infrastructure in academic organizations so that firewalls support availability and robustness of services. Firewalls don't against information publishing and communication among the people who would like to communicate.

It is possible to build a secure subnet or local area network out of a set of segments that each has mutually trusting machines. However, from a practical standpoint all but the most paranoid end users find this acceptable<sup>2</sup>. This is not a countermeasure against insider threats. Secondly, this option really obstructs openness.

DECISION: Systems, where student records, financial information, etc are processed, should be isolated from the main campus network by placing them behind firewalls.

Computer engineering community usually wants to experiment with a wide variety of features of the network, and will tend to cause abnormal traffic in network.

DECISION: Network laboratory of computer engineering department should be placed behind an extra firewall, and this firewall should have traffic rate limiting utility which controls the amount of packet traffic.

Additionally, academic organizations often have independent departmental budgets and semi-autonomous use of the campus network, which makes it difficult to enforce a common security approach. If one department in the university installs a security system that interferes with the others, they can and will simply purchase new network links to bypass it. One approach that seems to be for academia is to isolate critical computing systems behind internal firewalls.

DECISION: Network security of academic organizations should be managed from just one authority.

---

<sup>2</sup>D. Atkins, P. Buis, "Internet Security Professional Reference", New Riders

## Chapter 7

### CASE STUDY: FIREWALL DESIGN FOR IYTE

In this chapter, an academic firewall is described for IYTE. This firewall is designed by considering IYTE needs, environment, infrastructure, and threats against IYTE. Attacks against IYTE or other academic environment aren't analyzed for all known methods of attack are considered as a threat and this consideration is implemented in design. This firewall should be tested to find out its weakness before implementation. Structure of the other academic environments may be different so that their firewall design should be different.

#### 7.1.Design Principles

##### 7.1.1 Least privilege

The principle of least privilege is to have the minimum privileges necessary to perform assigned task and no more. Firewall components should be configured so they require as little privilege as possible. These are "blocking all packets not specifically allowed by one of the preceding rules", "building bastion hosts" and "disallowing users to access unnecessary services".

##### 7.1.2 Defense in depth

The principle of defense in depth is to increase number of the walls according to the increase of the security. Internal hosts are protected from the outside world by the exterior and interior firewalls. Web and FTP servers are protected exterior firewall.

##### 7.1.3 One Gate

The principle of one gate utilizes applying security policy and control. Everything between internal clients and the Internet comes through the perimeter net.

##### 7.1.4 Weakest link

The power of the security depends on weakest link. Allowing RPC and allowing any service to access internal network creates weak links. To allow RPC turns firewall to be nonoperational.

##### 7.1.5 Information Sharing

IYTE is an academic environment so that IYTE should publish in Internet as much as it can do. Information sharing depends on client behaviors, but that require some user education about the goals of and the need for the security measures which are adopted. Firewall rules should allow information sharing.

##### 7.1.6 Simplicity

Simplicity is important security strategy. This particular firewall configuration provides simplicity by separating components so that each component is as simple and comprehensible as possible. Blocking specific ports, rather than blocking all ports by default and then allowing specific ports, is a dangerous strategy. It's hard to develop and maintain a complete list of ports that need to be blocked at internal network. It would be better to block everything by default and then allow only specific ports. This increases simplicity.

## 7.2 Countermeasures and Assets Decision Table

In countermeasures against threats and assets chapter of thesis, each item is ended with a decision. These decisions provide a path to build firewall rules as shown in Table 7.1. Some decisions require different security tool other than firewalls. Needed security tool, place of firewall and applied firewall rule name, and are shown in this table. If counter-measure needs another security tool except firewalls, security tool is just written in "Security Tool" column of Table 7.1. So that there is no firewall rule for these items. It is shown in Table 7.2 and Table 7.3 how rule groups of firewall are implemented. High Availability and Easy of Use decisions are supported by all internal and external firewall rules, so that "All Rules" is written in rule group of firewall column in Table 7.1.

**Table 7.1 Countermeasures and Assets Decision Table**

	Decision	Security Tool	Place of Firewall	Rule Group of Firewall
<b>Countermeasures Against Threats</b>				
<b>Port Scanning</b>				
1.	Block unassigned port traffics.	Firewall	Int/Ext Firewall	Default
<b>Packet Sniffers</b>				
1.	Use strong authentication mechanism.	Authentication	-	-
2.	Use switched infrastructure if possible.	Physical sec	-	-
3.	Use cryptographically secure channel.	Privacy	-	-
<b>IP Spoofing</b>				
1.	If the source address of the incoming packet is an address which is belong to the internal address, block this datagram.	Firewall	Int/Ext Firewall	Spoofing
2.	Advice ISP to use RFC 2827 filtering.	Firewall	Ext Firewall	Spoofing
3.	Use Network Address Translation (NAT) and NAT reserved IP addresses for internal network..	Int Firewall OS	-	-
4.	Don't let IP addresses which is reserved for NAT go out and in.	Firewall	Int/Ext Firewall	Default
5.	Use cryptographic authentication.	Authentication	-	-
<b>TCP SYN Flood</b>				
1.	Check source address for going out packets source addresses and block packets which don't belong to internal network.	Firewall	Int/Ext Firewall	Spoofing
2.	Use SYN flood resistant firewall.	Int/Ext Firewall	-	-
<b>Ping of Death</b>				
1.	Use OS patch which is strong to the ping of death.	Bastion/Firewall OS	-	-
2.	Block fragmented packets.	Int/Ext Firewall	Int/Ext Firewall	Default

**Table 7.1 Countermeasures and Assets Decision Table (cont.)**

Decision		Security Tool	Place of Firewall	Rule Group of Firewall
<b>Smurf Attack</b>				
1.	Block IP-broadcast packets.	Firewall	Int/Ext Firewall	Default
2.	Disable echo services on the host and filter them at the firewall or Internet gateway.	Firewall	Int/Ext Firewall	Default
<b>Email Bombing and Spamming</b>				
1.	Use Intruder Detection System.	IDS	-	-
<b>Password Attacks</b>				
1.	Use One Time Password and/or cryptographic authentication.	Authentication	-	-
<b>Man-in-the-Middle Attacks</b>				
1.	Use cryptographic session.	Privacy	-	-
<b>Hijacking</b>				
1.	Use end-to-end integrity protection	Authentication	-	-
<b>Predicting TCP Initial sequence numbers</b>				
1.	Use OS patch against predictable TCP Initial Sequence numbers.	Firewall OS	-	-
2.	Encrypt TCP/IP data.	Privacy		
<b>Replay Attack</b>				
1.	Use OS patch against predictable TCP Initial Sequence numbers.	Authentication	-	-
2.	Encrypt TCP/IP data.	Privacy	-	-
<b>Application Layer Attacks</b>				
1.	Use Intruder Detection System.	IDS	-	-
<b>Network Scanners</b>				
1.	Use Intruder Detection System.	IDS	-	-
<b>DNS Security Problems</b>				
1.	Use Intruder Detection System.	IDS	-	-
<b>Trust Exploitation</b>				
1.	Use privacy and authentication mechanism.	Privacy, Authentication	-	-
<b>Port Redirection</b>				
1.	Use Intruder Detection System.	Firewall	Int/Ext Firewall	Default
<b>Unauthorized Access</b>				
1.	Use privacy and authentication mechanisms.	Privacy, Authentication	-	-
2.	Don't manage servers remotely without SSH.	Admin education	-	-



**Table 7.1 Countermeasures and Assets Decision Table (cont.)**

Decision		Security Tool	Place of Firewall	Rule Group of Firewall
<b>Virus and Trojan Horse Applications</b>				
1.	Use updated anti-virus software.	Antivirus Software	-	-
2.	It is necessary to call attention to the users these	User education	-	-
<b>RPC</b>				
1.	Block all unnecessary UDP ports.	Firewall	Int/Ext Firewall	Default
2.	If it isn't necessary, don't use RPC service.	Administration	-	-
<b>Insiders</b>				
1.	Authenticated and encrypted LAN infrastructure should be built.	Physical security	-	-
2.	It is necessary to inform users about network security and security personnel have to check the physical network infrastructure.	User education	-	-
<b>Assets and Needs of Academic Environment Network</b>				
<b>Electronic Mail</b>				
1.	Email service is needed by academicians and they need to access their mail system remotely in a secure way.	Firewall, Privacy	Int/Ext Firewall, Privacy	Mail POP server
2.	Email servers are target of DoS.	IDS	-	-
<b>Network News Transfer Protocol (NNTP)</b>				
1.	Private news groups and public news groups should be separated each other. Each one should have their own servers.	Firewall	Ext Firewall	NNTP Server
<b>Real Time Conferencing Services</b>				
1.	Real Time Conferencing Services have no security.	-	-	-
<b>World Wide Web (WWW)</b>				
1.	Academicians and other people want to use WWW service and academicians also want to update their web pages.	Firewall	Ext Firewall	HTTP Server
2.	WWW servers are target of DoS.	IDS	-	-
<b>File Transfer (FTP, TFTP)</b>				
1.	Academicians and other people want to use FTP service and academicians also want to update their files.	Firewall	Ext Firewall	FTP Server
2.	FTP and TFTP servers are target of DoS.	IDS	-	-
3.	TFTP server shouldn't open to the public.	Firewall	Int/Ext Firewall	Default

**Table 7.1 Countermeasures and Assets Decision Table (cont.)**

Decision		Security Tool	Place of Firewall	Rule Group of Firewall
<b>NFS</b>				
1.	NFS service shouldn't open to the public.	Firewall	Int/Ext Firewall	Default
<b>Domain Name Servers</b>				
1.	DNS servers are target of DoS.	IDS	-	-
<b>Password and Key servers</b>				
1.	Password and Key servers should be placed in a controlled area. They should be open for remote and local trusted users .	Firewall	Int/Ext Firewall	Kerberos Authentication Server
2.	Password and Key servers are target of DoS.	IDS	-	-
<b>Routers</b>				
1.	Routers are target of IPspoofing and DoS	IDS	-	-
2.	Routers should have robust software.	Router OS	-	-
<b>Firewalls and Intrusion Detection Systems</b>				
1.	Firewalls and IDS are target of DoS.	-	-	-
<b>Remote access</b>				
1.	Remote access via Telnet is necessary in a secure way.	Firewall	Int/Ext Firewall	SSH Server
<b>Information Transactions</b>				
1.	Private information transactions and public information transactions should be separated each other. They should have their own servers.	Administration	-	-
2.	Administrative information is vulnerable so it should be placed in private network No one can access this information remotely.	Firewall	Int/Ext Firewall	Default
3.	Less sensitive information may placed out of internal network.	Administration	-	-
<b>High Availability</b>				
1.	An appropriate balance is needed between high availability and security control.	Firewall	Int/Ext Firewall	All Rules
<b>Ease of Use</b>				
1.	The combination of approaches shows that an appropriate balance is needed between security and easy of use for academic environment.	Firewall	Int/Ext Firewall	All Rules

**Table 7.1 Countermeasures and Assets Decision Table (cont.)**

Decision		Security Tool	Place of Firewall	Rule Group of Firewall
<b>Openness</b>				
1.	Systems where student records, financial information etc. are processed should be isolated from the main campus networks by placing them behind firewalls.	Firewall	Int Firewall	Default
2.	Network laboratory of computer engineering department should be placed behind an extra firewall, and this firewall should have traffic rate limiting utility which controls the amount of packet traffic.	Firewall	Network Lab. Firewall	Traffic Rate Limiting Utility
3.	Network security of academic organizations should be managed from just one authority.	Administration	-	-

### 7.3 Constitution of The Firewall Rules

The current network structure of IYTE which is currently working is illustrated in Figure 7.1. This structure doesn't compromise any firewall so assets of IYTE network may suffer all network threats.

The services that users of IYTE are going to access through these firewalls are HTTP, terminal access, file transfer, electronic mail, Real Audio, Gopher, Wais, IRC, ICQ, Authentication Server access, news, DNS. All of these services are external services which are other sites support. If IYTE supports these services, users of IYTE can naturally access these services.

The hybrid and screened subnet architecture, described in Fundamentals of Firewalls chapter is used. Because this architecture provides better security than the other architectures. IYTE interior firewall rules block all access to the internal network. Serves as IYTE's main point of contact with the outside world are placed behind the exterior firewall in De-Militarized Zone (perimeter network). Exterior firewall protects servers. Each server runs a specific service. Thus, potential risk is divided in parts. RFC 2196 advice that "If possible, each service should be running on a different machine whose only duty is to provide a specific service. This helps to isolate intruders and limit potential harm.<sup>1</sup>". For servers run just their services, it is possible to configure the servers as bastion host servers. Each bastion host fulfills a specific role, all unnecessary services, protocols, programs, and network ports are disabled or removed. If bastion hosts are placed behind the interior firewall a security breach on the bastion host will immediately affect internal network. It is possible to use external router as an external firewall if router has firewall software. But external router of IYTE cannot be used as an external firewall for dial-up server of IYTE can't be placed in perimeter network. This causes modem back door for hosts which is settled in perimeter network.

Two kind of firewall designed for IYTE as depicted In Figure 7.2 and Figure 7.3 Both of them have De-Militarized Zone (DMZ). Figure 7.3 configuration let each faculty able to build their own public server. Although this alternative provides flexibility, it hindrances to build secure campus network. Each faculty just assembles secure local network for own faculty. This security can't be expanded for information belonging to secure zone have to pass through DMZ. Figure 7.2 alternative is preferable for it is possible to set up a secure server anywhere in campus. Figure 7.4 depicts this alternative descriptively. Each faculty and each user can publish their public data in WWW and FTP server where are settled in DMZ. So that packet filtering rules is generated for this alternative.

IYTE users cannot access their internal data which are kept in their offices, etc. from outside via Internet or dial-up server. If IYTE users put their private data in secure www and FTP server settled perimeter network, they can access their private data from anywhere. Before users access their private data in perimeter network, users must be

---

<sup>1</sup> B. Fraser, "Site Security Handbook", RFC 2196

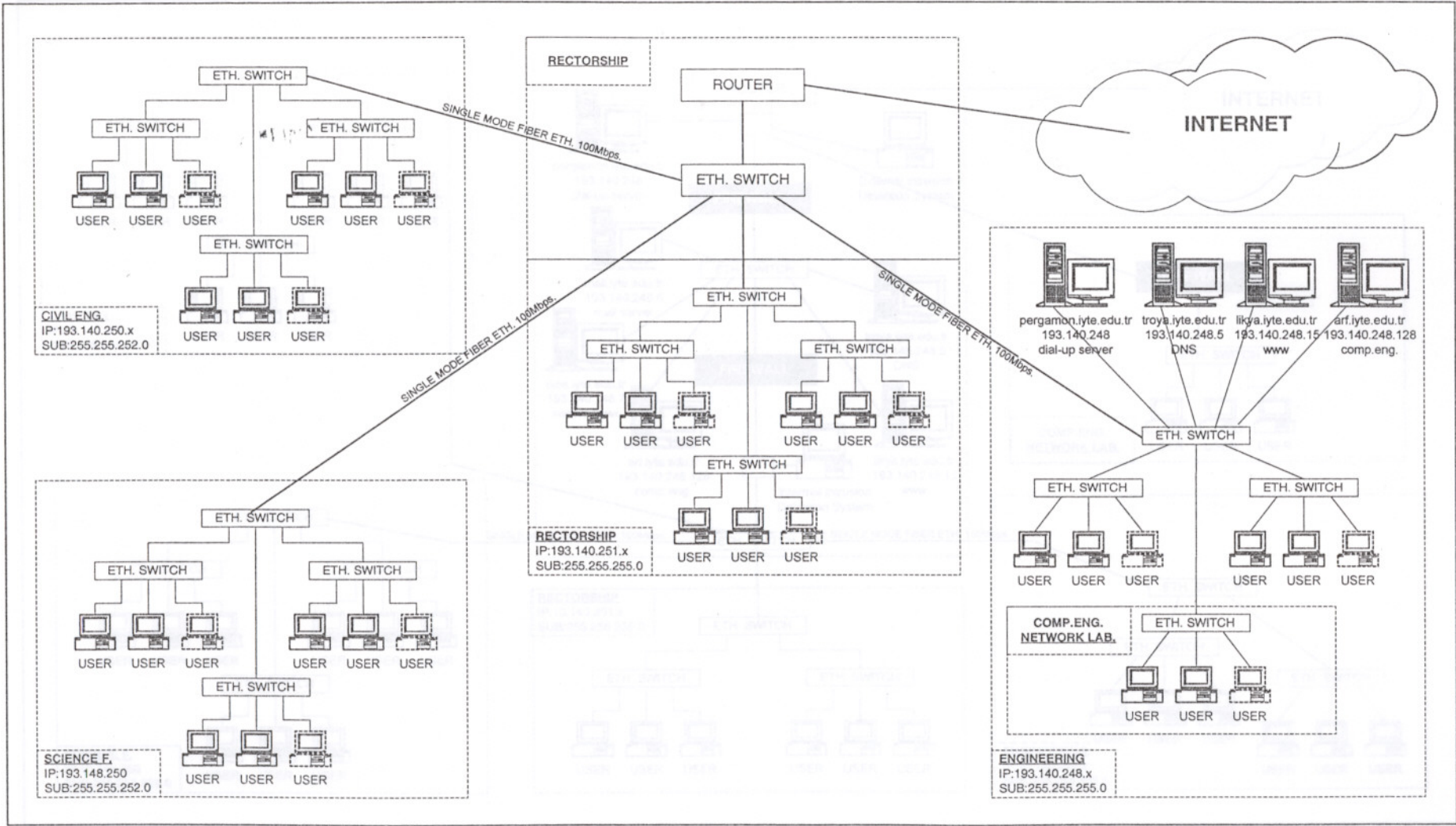


Figure 7.1 Network Infrastructure of IYTE Campus .

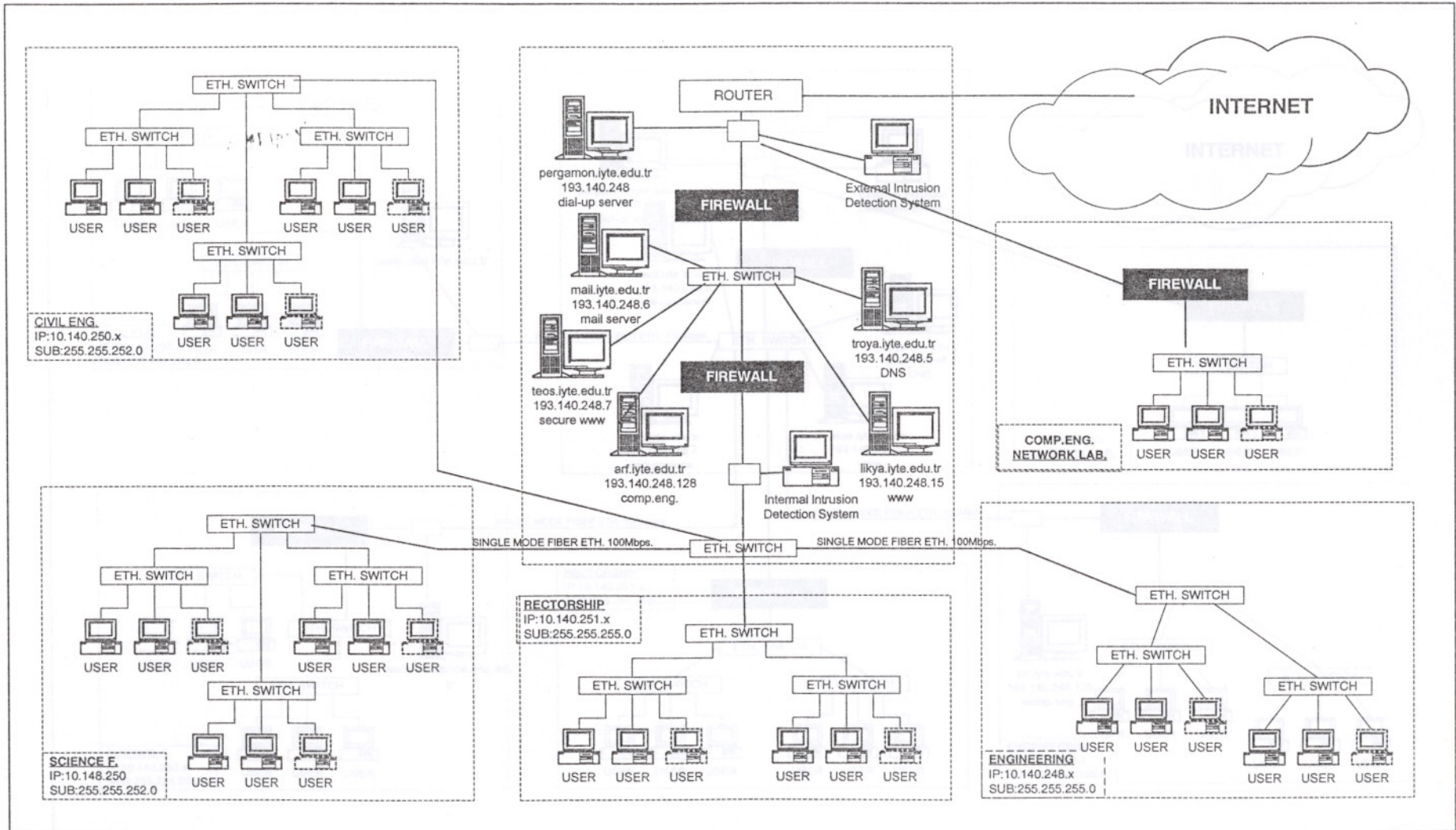


Figure 7.2 Firewall Implementation-A for IYTE Campus.

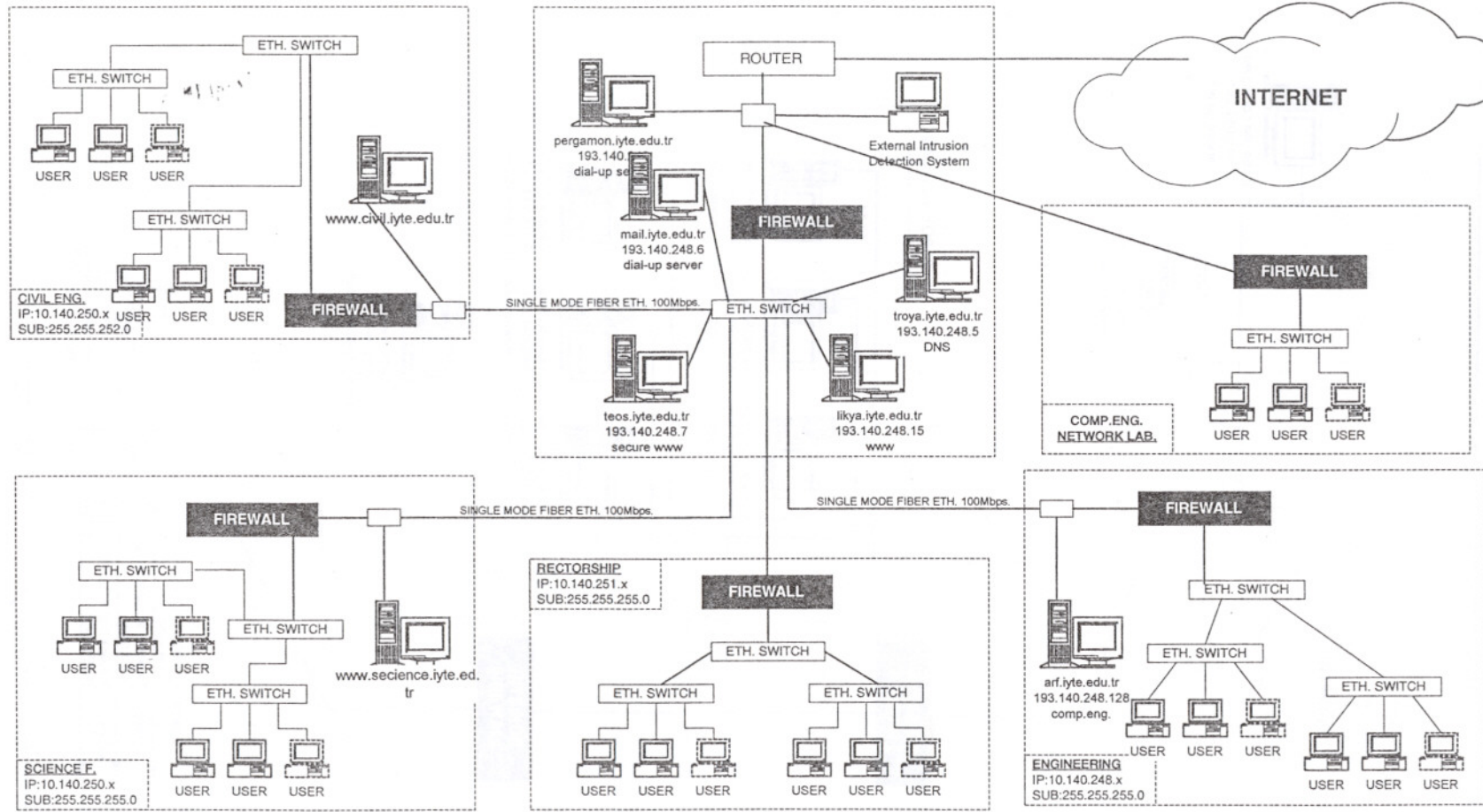


Figure 7.3 Firewall Implementation-B for IYTE Campus.

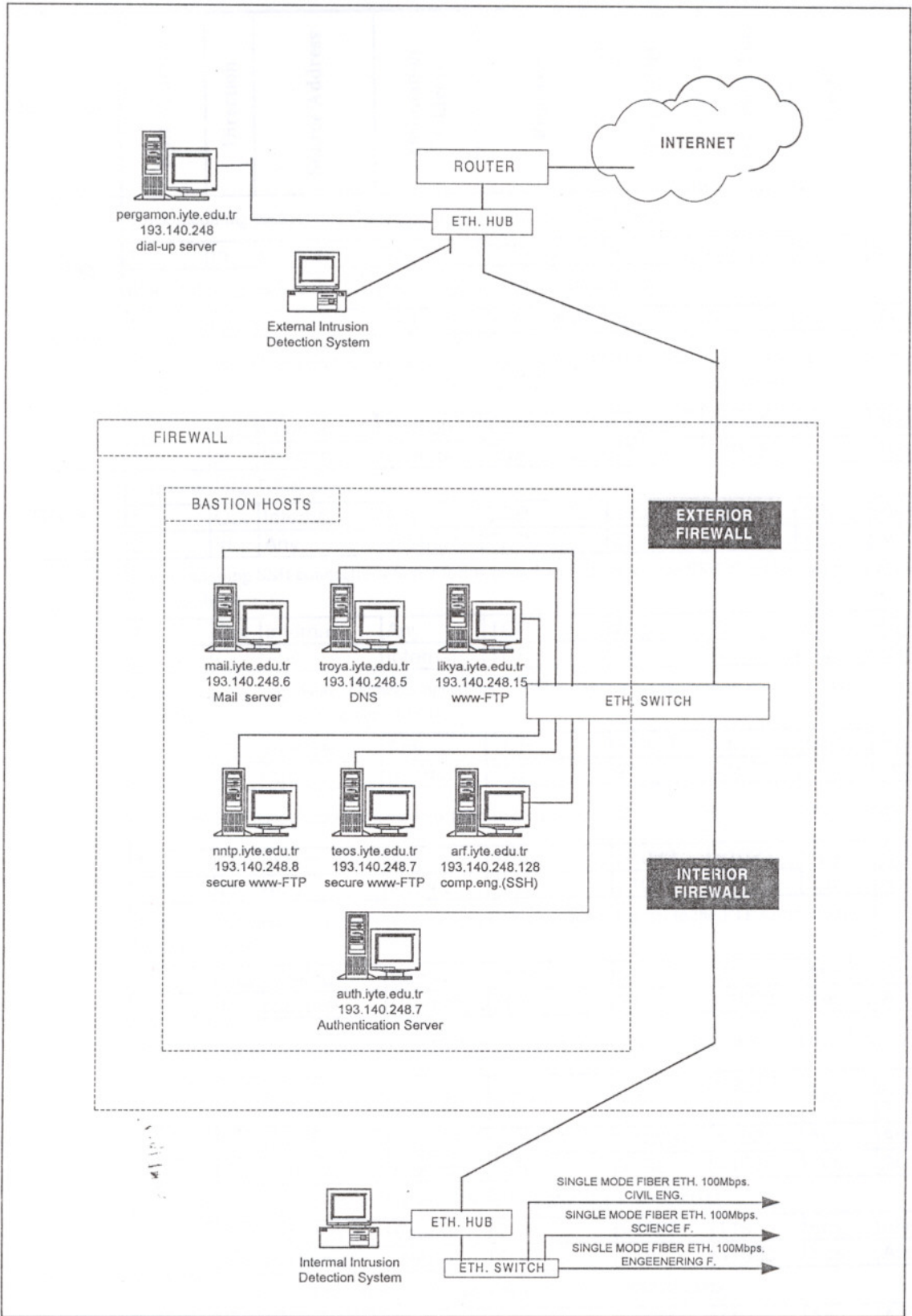


Figure 7.4 Detailed View of Firewall-A



**Table 7.2 IP Filter Configuration of Interior Hybrid Firewall**

Rule Group	Rule Number	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	ACK set	Action
Spoofing	Block incoming packets that claim to come from internal IP addresses.								
	1	In	Internal	Any	TCP - UDP	Any	Any	Any	Block
	Block outgoing packets that claim to come from external IP addresses.								
HTTP	1	Out	Internal	Bastion	TCP	>1023	80, 443	Any	Allow
	2	In	Bastion	Internal	TCP	80, 443	>1023	Yes	Allow
	Allow internal HTTP clients to connect to any HTTP and HTTPS server which is outside via caching bastion host . The connection from the client to the HTTP server will be over port 80.								
Telnet	Allow outgoing Telnet connections.								
	1	Out	Internal	Any	TCP	>1023	23	Any	Allow
	2	In	Any	Internal	TCP	23	>1023	Yes	Allow
SSH	Allow outgoing SSH connections. Some forms of authentication require SSH clients to use ports at or below 1023 or above.								
	1	Out	Internal	Any	TCP	Any	22	Any	Allow
	2	In	Any	Internal	TCP	22	Any	Yes	Allow
FTP	Allow outgoing command-channel connections to FTP servers, for use by passive-mode internal clients that are interacting with those servers directly.								
	1	Out	Internal	Any	TCP	>1023	21	Any	Allow
	2	In	Any	Internal	TCP	21	>1023	Yes	Allow
	Allow the FTP data channel connections from passive-mode internal clients to external FTP servers.								
	1	Out	Internal	Any	TCP	>1023	>1023	Any	Allow
	2	In	Any	Internal	TCP	>1023	>1023	Yes	Allow
	Allow normal internal FTP clients to open an FTP command channel to the FTP server on the bastion host.								
	1	Out	Internal	Bastion	TCP	>1023	21	Any	Allow
	2	In	Bastion	Internal	TCP	21	>1023	Yes	Allow
	Allow FTP data connections from the FTP server on the bastion host to non-passive internal clients.								
	1	In	Bastion	Internal	TCP	Any	6000-6020	Any	Block
2	In	Bastion	Internal	TCP	>1023	>1023	Any	Allow	
3	Out	Internal	Bastion	TCP	>1023	>1023	Yes	Allow	
NNTP	Allow outgoing news from internal users to service provider's news server.								
	1	Out	Internal	External	TCP	>1023	119	Any	Allow
	2	In	External	Internal	TCP	119	>1023	Yes	Allow
	Allow incoming news from service provider's news server to internal users.								
	1	In	External	Internal	TCP	>1023	119	Any	Allow
2	Out	Internal	External	TCP	119	>1023	Yes	Allow	

**Table 7.2 IP Filter Configuration of Interior Hybrid Firewall (cont.)**

Rule Group	Rule Number	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	ACK set	Action
Mail POP	Allow outgoing mail from internal users.								
	1	Out	In	External	TCP	>1023	110,109	Any	Allow
	2	In	Out	Internal	TCP	110,109	>1023	Yes	Allow
	Allow outgoing mail from internal users over SSL.								
	1	Out	Internal	External	TCP	>1023	110,109	Any	Allow
	2	In	External	Internal	TCP	995	>1023	Yes	Allow
	Allow incoming mail from external sender.								
	1	In	External	Internal	TCP	>1023	110,109	Any	Allow
	2	Out	Internal	External	TCP	110,109	>1023	Yes	Allow
	Allow incoming mail from external sender over SSL.								
REAL AUDIO	Allow outgoing Real Audio connections.								
	1	Out	Internal	External	TCP	>1023	7070	a	Allow
	2	In	External	Internal	TCP	7070	>1023	Yes	Allow
	3	In	External	Internal	UDP	6970-7170	>1023	a	Allow
GOPHER	Allow outgoing Real Gopher connections.								
	1	Out	Internal	External	TCP	>1023	70	Any	Allow
	2	In	External	Internal	TCP	70	>1023	Yes	Allow
WAIS	Allow outgoing WAIS connections.								
	1	Out	Internal	External	TCP	>1023	210	Any	Allow
	2	In	External	Internal	TCP	210	>1023	Yes	Allow
IRC	Allow internal IRC clients to contact external IRC clients over external servers.								
	1	Out	Internal	External	TCP	>1023	6667	Any	Allow
	2	In	External	Internal	TCP	6667	>1023	Yes	Allow
	Allow internal IRC clients to contact external IRC clients.								
	3	In	External	Internal	TCP	>1023	>1023	Any	Allow
4	Out	Internal	External	TCP	>1023	>1023	Yes	Allow	
Kerberos Authentication Server	Allow internal user to access bastion and other external authentication server.								
	1	Out	Internal	External	UDP	>1023	88	a	Allow
	2	In	External	Internal	UDP	88	>1023	a	Allow
ICQ	Allow internal ICQ clients to contact external ICQ clients over external servers.								
	1	Out	Internal	ICQ server	UDP	>1023	4000	a	Allow
	2	In	ICQ server	Internal	UDP	4000	>1023	a	Allow
	3	Out	Internal	ICQ serv.	TCP	>1023	>1023	Any	Allow
	4	In	ICQ server	Internal	TCP	>1023	>1023	Yes	Allow
	Allow internal ICQ clients to contact external ICQ clients.								
	5	Out	Internal	External	TCP	>1023	>1023	Any	Allow
	6	In	External	Internal	TCP	>1023	>1023	Yes	Allow
7	Out	External	Internal	TCP	>1023	>1023	Any	Allow	
8	In	Internal	External	TCP	>1023	>1023	Yes	Allow	

**Table 7.2 IP Filter Configuration of Interior Hybrid Firewall (cont.)**

Rule Group	Rule Number	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	ACK set	Action
DNS	Allow UDP-based DNS queries and answers from the internal DNS server to the bastion host DNS server.								
	1	Out	Internal DNS server	Bastion	UDP	53	53	a	Allow
	Allow UDP-based DNS queries and answers from the bastion host DNS server to the internal DNS server.								
	1	In	Bastion	Internal DNS server	UDP	53	53	a	Allow
	Allow TCP-based DNS queries from the internal DNS server to the bastion host DNS servers, as well as answers to those queries. Also allow zone transfers in which the bastion host DNS server is the primary server and the internal DNS server is the secondary server.								
	1	Out	Internal DNS server	Bastion	TCP	>1023	53	Any	Allow
	2	In	Bastion	Internal DNS server	TCP	53	>1023	Yes	Allow
	Allow TCP-based DNS queries from the bastion host DNS server to the internal DNS server; as well as answers to those queries. Also allow zone transfers in which the bastion host DNS server is the secondary server and the internal DNS server is the primary server.								
Default	5	In	Bastion	Internal DNS server	TCP	>1023	53	Any	Allow
	6	Out	Internal DNS server	Bastion	TCP	53	>1023	Yes	Allow
	Block all packets not specifically allowed by one of the preceding rules.								
Default	1	Out	Any	Any	TCP - UDP	Any	Any	Any	Block
	2	In	Any	Any	TCP - UDP	Any	Any	Any	Block

İZMİR YÜKSEK TEKNOLOJİ ENSTİTÜSÜ  
REKTÖRLÜĞÜ  
Kütüphane ve Dokümantasyon Daire Bşk

**Table 7.3 IP Filter Configuration of Exterior Hybrid Firewall**

Rule Group	Rule Number	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	ACK set	Action
Spoofing	Block incoming packets that claim to come from internal IP addresses.								
	1	In	Internal	Any	TCP - UDP	Any	Any	Any	Block
	Block outgoing packets that claim to come from external IP addresses.								
	1	Out	External	Any	TCP - UDP	Any	Any	Any	Block
	Block incoming packets that claim to come from DMZ IP addresses.								
	1	In	Internal	Any	TCP - UDP	Any	Any	Any	Block
HTTP SERVER	Allow external clients to contact the bastion host HTTP server.								
	1	In	Any	Bastion	TCP	>1023	80, 443	Any	Allow
	2	Out	Bastion	Any	TCP	80, 443	>1023	Yes	Allow
	Allow bastion host HTTP server to contact the external any HTTP server for caching.								
	1	Out	Bastion	Any	TCP	>1023	80,443	Any	Allow
	2	In	Any	Bastion	TCP	80,443	>1023	Yes	Allow
SSH SERVER	Allow bastion SSH connections.								
	1	In	Any	Bastion	TCP	Any	22	Any	Allow
	2	Out	Internal	Bastion	TCP	22	Any	Yes	Allow
FTP SERVER	Allow incoming FTP request and respond from FTP Bastion Host.								
	1	In	Any	Bastion	TCP	>1023	21	Any	Allow
	2	Out	Bastion	Any	TCP	21	>1023	Yes	Allow
	Allow the FTP data channel connections for incoming request and respond, normal-mode.								
	1	Out	Bastion	Any	TCP	20	>1023	Any	Allow
	2	In	Any	Bastion	TCP	>1023	20	Yes	Allow
	Allow the FTP data channel connections for incoming request and respond, passive-mode.								
	1	Out	Bastion	Any	TCP	>1023	20	Yes	Allow
2	In	Any	Bastion	TCP	>1023	21	Any	Allow	
Mail POP Server	Allow outgoing mail from Bastion POP Mail Server.								
	1	Out	Bastion	External	TCP	>1023	110,109	Any	Allow
	2	In	Out	Bastion	TCP	110,109	>1023	Yes	Allow
	Allow outgoing mail from Bastion Mail Server over SSL.								
	1	Out	Bastion	External	TCP	>1023	110,109	Any	Allow
	2	In	External	Bastion	TCP	995	>1023	Yes	Allow
	Allow incoming mail from external sender to Bastion POP mail server.								
	1	In	External	Bastion	TCP	>1023	110,109	Any	Allow
	2	Out	Bastion	Internal	TCP	110,109	>1023	Yes	Allow
	Allow incoming mail from external sender to the Bastion POP mail server over SSL.								
1	In	External	Bastion	TCP	>1023	110,109	Any	Allow	
2	Out	Bastion	External	TCP	995	>1023	Yes	Allow	
NNTP Server	Allow outgoing news from Bastion host news server.								
	1	Out	Bastion	External	TCP	>1023	119	Any	Allow
	2	In	External	Bastion	TCP	119	>1023	Yes	Allow
	Allow incoming news from other news serves to bastionhost news server.								
	1	In	External	Bastion	TCP	>1023	119	Any	Allow
	2	Out	Bastion	External	TCP	119	>1023	Yes	Allow

**Table 7.3 IP Filter Configuration of Exterior Hybrid Firewall (cont.)**

Rule Group	Rule Number	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	ACK set	Action
Kerberos Authentication Server	Allow internal user to access bastion and other external authentication server.								
	1	Out	Bastion	External	UDP	>1023	88	a	Allow
	2	In	External	Bastion	UDP	88	>1023	a	Allow
SECURE HTTP SERVER	Allow the bastion host HTTP server to connect to the HTTP and HTTPS servers on any machine on the Internet.								
	1	Out	Bastion	Any	TCP	>1023	Any	Any	Allow
	2	In	Any	Bastion	TCP	Any	>1023	Yes	Allow
	Allow external clients to contact the bastion host HTTP server.								
	1	In	Any	Bastion	TCP	>1023	80	Any	Allow
	2	Out	Bastion	Any	TCP	80	>1023	Yes	Allow
SECURE FTP SERVER	Allow incoming FTP request and respond from FTP Bastion Host.								
	1	In	Any	Bastion	TCP	>1023	21	Any	Allow
	2	Out	Bastion	Any	TCP	21	>1023	Yes	Allow
	Allow the FTP data channel connections for incoming request and respond, normal-mode.								
	1	Out	Bastion	Any	TCP	20	>1023	Any	Allow
	2	In	Any	Bastion	TCP	>1023	20	Yes	Allow
	Allow the FTP data channel connections for incoming request and respond, passive-mode.								
	1	Out	Bastion	Any	TCP	>1023	20	Yes	Allow
	2	In	Any	Bastion	TCP	>1023	21	Any	Allow
Interior Firewall Client Rules	Allow packets of client side which is placed back of interior firewall to get service from external servers. Use the same rules.								
	<b>HTTP, SSH, FTP, Mail POP, NNTP, Kerberos demands, ICQ, IRC, Telnet, Real</b>								
DNS	Allow UDP-based DNS queries and answers from the bastion host DNS server to DNS servers in the								
	1	Out	Bastion	Any	UDP	53	53	a	Allow
	Allow UDP-based DNS queries and answers from Internet DNS servers to the bastion host DNS server.								
	2	In	Any	Bastion	UDP	53	53	a	Allow
	Allow external UDP-based DNS clients to query the DNS server on the bastion host and it to answer								
	3	In	Any	Bastion	UDP	Any	53	a	Allow
	4	Out	Bastion	Any	UDP	53	Any	a	Allow
	Allow TCP-based DNS queries from the bastion host to DNS servers on the Internet, as well as answers to those queries. Also allow zone transfers in which the bastion host DNS server is the secondary server and an external DNS server is the primary server.								
5	Out	Bastion	Any	TCP	>1023	53	Any	Allow	
6	In	Any	Bastion	TCP	53	>1023	Yes	Allow	
Allow TCP-based DNS queries from the outside world to the bastion host DNS server, as well as									
*7	In	Any	Bastion	TCP	>1023	53	Any	Allow	
8	Out	Bastion	Any	TCP	53	>1023		Allow	
Default	Block all packets not specifically allowed by one of the preceding rules.								
	1	Out	Any	Any	TCP - UDP	Any	Any	Any	Block
	2	In	Any	Any	TCP - UDP	Any	Any	Any	Block

authenticated by authentication server settled perimeter network. Thus mobile users of IYTE academic environment can access their private data anywhere.

In internal network, there is no real IP address. Machines have private addresses. These addresses reserved for internal usage by IETF. Using these addresses get extra security. Because private addresses have no global meaning, routing information about private networks shall not be propagated on inter-enterprise links, and packets with private source or destination addresses should not be forwarded across such links. Routers in networks not using private address space, especially those of Internet service providers, are expected to be configured to reject (filter out) routing information about private networks. If such a router receives such information the rejection shall not be treated as a routing protocol error.<sup>2</sup>

## **7.4 Components of IYTE Firewall**

### **7.4.1 HTTP Server**

IYTE firewall provides two kinds of HTTP service. IT allows internal users to access other people's web sites, and users want to put up IYTE web site. Firewall could simply allow internal hosts to create connections to port 80, port 443. That will allow access to almost any HTTP or HTTPS server and will also be useful for supporting FTP. If a caching proxy server is used, HTTP performance is significantly improved for internal HTTP clients. Clients obtain pages from the cache over the internal network, rather than from the original server over Internet connection, which is probably much slower so that interior firewall rules force interior clients to access outside web pages via HTTP server. HTTPS connections can't be cached because the encryption means that pages are different every time they're accessed, but a caching proxy server won't interfere with HTTPS service; it will simply act like a normal proxy. And it is possible to separate caching HTTP server and publishing HTTP server. All clients publish their information on public HTTP server after they authenticated. Secure HTTP server provides secure access to the clients. Each client accesses this server from internal network or Internet.

### **7.4.2 Mail Server**

There are many options for mail in any configuration. POP mail more trusted and manageable than SMTP. So that using POP mail is more convenient than SMTP. It has also SSL option for secure mail. Clients can do all external mail connections to go to a single machine with a bastion mail server.

### **7.4.3 Telnet**

Outgoing Telnet is provided through firewall. This is not harmful for internal network. Incoming Telnet is considerably more difficult to provide safely and conveniently. If it were necessary, incoming Telnet could be provided on the bastion

---

<sup>2</sup> Y. Rekhter, "Address Allocation for Private Internets", RFC 1918, p. 4

host using extra authentication. It is reasonable to disallow incoming Telnet altogether, replacing it with SSH.

#### **7.4.4 SSH Server**

Although incoming Telnet is unsafe, it's useful to be able to allow some form of remote access. The safest way to do so is to allow bastion SSH server. The SSH server should be safely configured. On the other hand, it requires having user accounts configured on the bastion host. If only a few users need to use SSH, it may be the best way not to provide the service. Firewall also allows outgoing SSH.

#### **7.4.5 FTP**

FTP doesn't lend itself to a pure packet filtering solution. Because normal-mode FTP requires an incoming connection to an arbitrary port over 1023, trying to allow it without doing anything else gives intruders access to all kinds of services running on internal systems. So that supporting only passive mode via packet filtering brings more security. Disallowing doesn't effects clients because some popular FTP clients-the ones built in to Web browsers like Netscape Navigator or Internet Explorer use passive mode without being modified. Bastion FTP server and internal clients can communicate non-passive mode. Because firewall can control FTP packets coming from bastion FTP by checking IP address. All clients publish their information on FTP server after they authenticated. Secure FTP server provides secure access to the clients. Each client accesses this server from internal network or Internet.

#### **7.4.6 NNTP Server**

Building a news server on the bastion host is safe. News servers fail with dreary regularity, while the problems usually aren't security- related.

#### **7.4.7 Authentication Server (Kerberos)**

Secure HTTP-FTP server and mail server need to be authenticated when some IYTE client want to access his or her information. This is checked by any authentication server. In this thesis Kerberos Authentication Server is chosen for it is widely used in academic environment. All clients will be authenticated by authentication server whenever they want to access internally or externally.

#### **7.4.8 DNS Server**

DNS is best provided across a firewall with a pair of servers: one on the bastion host, the other on an internal host. DNS presents a situation in which the number of rational solutions is clearly limited. It is needed to decide whether to use separate internal and external servers to do information hiding, or whether the external world should be allowed to see all of the host data. There is no need to hide DNS information. For IYTE, the DNS server on the bastion host is secondary server for IYTE domain, and that the primary server is on an internal host.

## 7.4.9 Packet Filtering Rules

Based on the configuration decisions table, packet-filtering rules are derivated. The derivated rules are shown Table 7.2. and Table 7.3. Packet filtering system can distinguish between incoming and outgoing packets and it can filter on source address, destination address, packet type (TCP or UDP), source port, destination port and setting of ACT bit (for only TCP). Additionally packet filter has capability to apply rules in the order listed.

## 7.4.10 Interior Firewall

The purpose of the interior firewall is to protect the internal network from the Internet and from bastion host. The interior firewall is a hybrid firewall. The rules and descriptions of interior firewall are shown in Table 7.2. The rules are derivated from countermeasures and assets decision table.

## 7.4.11 Exterior Firewall

The purpose of the exterior firewall is to protect the perimeter net and the internal net against the outside world. The differences between the rules for the interior firewall and the exterior firewall all have to do with the bastion host. That's because the bastion host sits outside of the interior firewall. The rules and descriptions of exterior firewall are shown in Table 7-3. The rules are derivated from countermeasures and assets decision table.

## 7.4.12 Firewall of Computer Network Laboratory

Network Laboratory is a trial environment and any accidental incident may be occurred. So that network laboratory should be separated from Internet by a firewall. This environment needs any service of Internet. In this respect, packet filtering rules cannot be used in this firewall. But traffic rate limiting precautions should be taken for mitigating the risk of accidental incidents. This type of filtering limits the amount of nonessential traffic that crosses network segments to a certain rate. A common example is to limit the amount of ICMP traffic allowed into a network because it is used only for diagnostic purposes. ICMP-based DoS attacks are common.

## 7.5 Need of Authentication and Privacy

Threats and counter measures chapter of thesis expose that “privacy and authentication are the major problem of TCP/IPv4”<sup>3</sup>. Suggesting any authentication and privacy mechanism is beyond of this thesis. There are many privacy tool alternatives (such as S/MIME, PGP, SSL, HTTPS, PKI, Ipsec) and the authentication tools alternatives (such as S/Key, Kerberos and SecurID, PKI, IPsec). IPsec is more advanced than the others. IPsec was developed as IP level privacy mechanism so there is no need to change applications. IPsec is designed to provide interoperable, high quality, cryptographically based security for IPv4 and IPv6. The set of security services offered

---

<sup>3</sup> M. Goncalves, “Firewalls Complete”, McGraw-Hill Companies



includes access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.<sup>4</sup> Encryption is not necessary for internal packet transfer. The infrastructure of IYTE campus network has switch ethernet hardware so it is resist sniffing.

## 7.6 Need of Intruder Detection System

Threats and counter measures chapter of thesis expose the need of Intruder Detection System (IDS). A firewall is simply a fence around the private network. So that firewall has no capability of detecting intruder trying to break in, nor does firewall know if intruder coming through the firewall is allowed in. It simply restricts access to the designated points. IDS monitors packets on the network wire and attempts to discover if an intruder attempting to break into a system, so that intrusion detection system is necessary if there are already a firewall. IYTE campus network needs two IDS as shown in Figure 7.4. One of them is used for detecting internal attempts, the other for external attempts.

## 7.7 Need of Testing Firewall

Testing allows the actual security level of firewall to be compared with that desired.<sup>5</sup> If it isn't done by who build firewall, it will be done any intruder anyway. First firewall is checked for well-known security holes. There are penetration test tools like SATAN, Tiger, COPS and etc. which have capable to test the firewall. After testing, firewall should be reconfigured according to its recognized weakness.

---

<sup>4</sup> S. Kent, R. Atkinson, Security Architecture for the Internet Protocol , RFC 2401, November 1998,p 4

<sup>5</sup> S. Boran,"IT Security Cookbook ", [http://secinf.net/info/misc/boran/Firewalls\\_Securing\\_externalNetwork\\_connections.htm](http://secinf.net/info/misc/boran/Firewalls_Securing_externalNetwork_connections.htm)

## Chapter 8

### CONCLUSION

The only way to truly secure the computer is to isolate it from non-secured networks. Academic organizations increasingly need that Internet connection is becoming a vital requirement. Connecting Internet and being exposed to network attacks are natural result for an academic organization. Network attacks can be as varied as the systems that they attempt to penetrate. Some limitations of the TCP/IP protocol are evaluated by the types of attacks. When the Internet was formed, it linked various government entities and universities to one another with the express purpose of facilitating learning and research. The original architecture of the TCP/IP never has been designed to aim security. For this reason, most TCP/IP implementations are inherently insecure.

So need of information and security causes an appropriate balance between security and availability in an academic environment. Firewalls, Intrusion Detection Systems, Privacy and Authentication Systems are non-abandonable tools to build a secure environment. Year by year, new threats and new countermeasures will conflict each other.

Firewalls, especially screened subnet hybrid architecture relatively gets good security by controlling the packet traffic. The most important thing to building a firewall is to put the rules. Rules represent the security level. Any wrong rule may open a big leak in security. For that reason, constructing a secure zone as shown in case study, is the best practical method. Thus information can be transacted in internal network with less worry. Screened subnet firewall architecture also permits perimeter network. Perimeter network in other word DMZ is a meeting point for external and internal network. The main potential disadvantages of designed firewall are clients cannot access their desktops from Internet, but this need is supplied by a secure www-FTP server. Only one DMZ may be sufficient today. In the future, it may be necessary to build DMZ for each faculty. But multi DMZ would enhance the management complexity. It would be relatively easy to construct a more secure configuration with the same basic architecture would be a more complex and fragile configuration. Designed firewall doesn't prohibit to access external resources. But incoming packets are dropped unless they can be directly linked to a request originating inside the firewall. Usage of expendable hosts and conscious selection and physical separation of public data and private data is the most critical factor to success security.

As a consequence, the designed firewall is largely transparent to trusted users and therefore retains the sense of "openness" critical in an academic environment. This transparency and perceived openness actually increase security by eliminating the desire for users to bypass security mechanisms.

Although the threats chapter of thesis proves needs of privacy and authentication, Privacy and Authentication mechanisms aren't scope of this thesis. Thus this thesis may lead to analyzing and implementing privacy and authentication mechanisms in an academic environment as a future work.

## SUMMARY

Computer Networks in academic environments could have many security problems if there weren't enough precaution. The source of these problems is generally vulnerability of TCP/IP protocol and Internet. Vulnerabilities cause threats. These threats can be summarized as port scanning, packet sniffers, IP spoofing, denial of service, password attacks, man in the middle attacks, hijacking, replay attack, application layer attacks, network reconnaissance, trust exploitation, unauthorized access, viruses and Trojan horse applications.

These threats endanger the assets of academic network. These assets are internal workstations, local data, survivability of services, Internet servers such as www, FTP, mail, and dns. And academic networks have different security needs because of different characteristic properties from other environments such as banking or military. Most important property of an academic environment is openness. Openness and security conflict each other. Firewalls balance this confliction.

Firewalls are a kind of security tool to be used for preventing the assets in the network. There are many kind of firewalls such as packet filters, dual-homed host, proxy systems, screened host, screened subnet. In case study, a screened subnet firewall is used for IYTE. All firewalls needs to know what they do. Design basis of Firewall can be summarized as follows:

- a. Determine the threats
- b. Determine the assets and system needs
- c. Constitute the firewall rules according to threats and system needs.

The firewall rules of academic environment block external access to the private network, allow private network clients to access external and internal resources. All Internet users can access public information of academic environment. Clients of academic environment can access their own private information by Internet. The designed firewall relatively lessens the potential harm of network threats.

## ÖZET

Gerekli önlemler alınmaz ise, akademik ortamlardaki bilgisayar ağlarının birçok güvenlik problemi bulunabilir. Bu problemlerin çoğu TCP/IP protokolünün ve Internet'in zayıflıklarından kaynaklanmaktadır. Zayıflıklar tehditlere sebep olur. Bu tehditler, port tarayıcı, paket sniffers, IP spoofing, hizmet dışı bırakma, password saldırıları, ortadaki adam saldırıları, hijacking, tekrarlanan saldırı, uygulama katmanı saldırıları, ağ keşfi güven istismarı, yetkisiz erişim, virüsler ve Truva atı uygulamaları olarak özetlenebilir.

Bu tehditler, akademik ağdaki değerli nesnelere tehlikeye sokar. Bu değerler, yerel iş istasyonları, yerel data, hizmetlerin devamlılığı, Internet sunucularıdır (www,FTP,dns gibi). Akademik ağlar, askeri yada bankacılık gibi ortamlardan farklı özelliklere sahip olduğundan, farklı güvenlik ihtiyaçları vardır. Akademik ortamın en önemli özelliği açıklıktır. Açıklık ve güvenlik birbiriyle çatışır. Firewall'lar bu çatışmayı dengeler.

Firewall'lar ağdaki değerleri korumak için kullanılan bir güvenlik aracıdır. Packet filter, dual-homed gateway, proxy system, bastion host gibi birçok çeşit firewall vardır. Bütün firewall'lar ne yapacaklarını bilmeye ihtiyaç duyarlar. Firewall'un tasarım esasları şöyle özetlenebilir:

- a. Tehditleri tespit etme
- b. Sistem ihtiyaçlarını ve değerlerini tespit etme
- c. Sistem ihtiyaçlarına ve tehditlere göre firewall kurallarını oluşturma

Akademik ortamın firewall kuralları özel ağa dışarıdan erişimi engeller, özel ağ kullanıcılarına dış ve iç kaynaklara erişmesine izin verir. Bütün Internet kullanıcıları akademik ortamın akademik ortamın herkese açık bilgilerine erişebilir. Akademik ortamın kullanıcıları kendi özel bilgilerine Internet ile erişebilirler. İkinci olarak Tasarlanan firewall ağdan kaynaklanan tehditlerin olası zararlarını nispeten azaltır.

## BIBLIOGRAPHY

- Anonymous, "Maximum Security", Macmillan Computer Publishing , 1998.
- Atkins D., Buis P., "Internet Security Professional Reference", New Riders, 1996.
- Boran S., "IT Security Cookbook ", [http://secinf.net/info/misc/boran/Firewalls\\_Securing\\_external\\_Network\\_connections.htm](http://secinf.net/info/misc/boran/Firewalls_Securing_external_Network_connections.htm), 1999.
- Chapman B., "Building Internet Firewalls", O'Reilly, 2000.
- Cheswick W., Bellovin S., "Firewalls and Internet Security", Addison-Wesley, 1994.
- Cormack A., "Web Security ", <http://www.jisc.ac.uk/acn/authent/cormack.html>, 1997.
- Curtin M., Ranum M., "Internet Firewalls: Frequently Asked Questions", <http://www.clark.net/pub/mjr/pubs/fwfaq/>, 1999.
- Ferguson P., Senie D., "Network Ingress Filtering", RFC 2827, 2000.
- Fraser B., "Site Security Handbook", RFC 2196, 1997.
- Goncalves M., "Firewalls Complete", McGraw-Hill Companies, 1998.
- Graham R., "Hacking Lexicon", <http://www.robertgraham.com/pubs/hacking-dict.html>, 2001.
- Howard J., "An Analysis Of Security Incidents On The Internet", <http://www.cert.org/research/JHThesis/Chapter16.html>, 1997.
- IBM Corp. , "Internet Security in the Network Computing Framework", IBM Corp., 1998.
- Kent S., Atkinson R., "Security Architecture for the Internet Protocol", RFC 2401, 1998.
- Maxon K. "Application Layer Firewalls vs. Network Layer Firewalls Which Is the Better Choice?", <http://www.secinf.net/info/fw/firewall.htm>, 2000.
- McGibbon S., "Firewalls and Internet Security", <http://www.secinf.net/info/fw/steph>.
- Pethia R., "Internet Security Trends", <http://www.cert.org/present/internet-security-trends/tsld008.htm>, 2001.
- Power R., "Current and Future Danger" , <http://www.gocsi.com/crreport.htm>, 1995.
- Ranum M., "Internet Firewalls Frequently Asked Questions", <http://www.clark.net/pub/mjr/pubs/fwfaq/>, 1999.

Rekhter Y., "Address Allocation for Private Internets", RFC 1918, 1996.

Safford D., "How to pick an Internet Firewall", Texas A&M University, USENIX Security Symposium, 1993.

Safford D., Schales D., Hess D., "The TAMU Security Package", USENIX Symposium, 1993.

Senie D., "Changing the Default for Directed Broadcasts in Routers", RFC 1812, 1999.

Shirey R., "Internet Security Glossary", RFC 2828, 2000.

Skoudis E., "Fire in the Hole,E. Skoudis", <http://www.seconf.net/info/fw/fire.htm>, 1998.

Sonnenreich W., Yates T., "Building Linux and OpenBSD Firewalls", Wiley, 2000.

Wack J., "Keeping Your Site Comfortably Secure: An Introduction to the Internet and Internet Security ", NITS Special Publications, 800-10, 1995.