2005-03

Evaluation of Embedded Firewall System

Rumelioglu, Sertac.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EVALUATION OF THE EMBEDDED FIREWALL SYSTEM

by

Sertac Rumelioglu

March, 2005

Thesis Advisor:	Su Wen
Second Reader:	Craig Martell

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Evaluation of the Embedded Firewall System			**5. FUNDING NUMBERS**
6. AUTHOR(S) **Sertac Rumelioglu**			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The performance aspect and security capabilities of the Embedded Firewall (EFW) system are studied in this thesis. EFW is a host-based, centrally controlled firewall system consisting of network interface cards and the "Policy Server" software. A network consisting of EFW clients and a Policy Server is set up in the Advanced Network Laboratory at the Naval Postgraduate School. The Smartbits packet generator is used to simulate realistic data transfer environment. The evaluation is performed centered on two main categories: performance analysis and security capability tests. TTCP program and a script written in TCL are used to perform throughput and packet loss tests respectively. The penetration and vulnerability tests are conducted in order to analyze the security capabilities of EFW. Symantec Personal Firewall is used as a representative application firewall for comparing test results. Our study shows that EFW has better performance especially in connections with high amounts of encrypted packets and more effective in preventing insider attacks. However, current implementation of EFW has some weaknesses such as not allowing sophisticated rules that application firewalls usually do. We recommend that EFW be used as one of the protection mechanisms in a system based on the defense-in-depth concept that consists of application firewalls, intrusion detection systems and gateway protocols.

14. SUBJECT TERMS Firewall, embedded firewall, firewall evaluation, firewall performance, defense-in-depth			**15. NUMBER OF PAGES** 97
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

EVALUATION OF EMBEDDED FIREWALL SYSTEM

Sertac Rumelioglu
Lieutenant Junior Grade, Turkish Navy
B.S., Turkish Naval Academy, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2005

Author: Sertac Rumelioglu

Approved by: Dr. Wen Su
Thesis Advisor

Dr. Craig Martell
Second Reader

Dr. Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The performance aspect and security capabilities of the Embedded Firewall (EFW) system are studied in this thesis. EFW is a host-based, centrally controlled firewall system consisting of network interface cards and the "Policy Server" software. A network consisting of EFW clients and a Policy Server is set up in the Advanced Network Laboratory at the Naval Postgraduate School. The Smartbits packet generator is used to simulate realistic data transfer environment. The evaluation is performed centered on two main categories: performance analysis and security capability tests. TTCP program and a script written in TCL are used to perform throughput and packet loss tests respectively. The penetration and vulnerability tests are conducted in order to analyze the security capabilities of EFW. Symantec Personal Firewall is used as a representative application firewall for comparing test results. Our study shows that EFW has better performance especially in connections with high amounts of encrypted packets and more effective in preventing insider attacks. However, current implementation of EFW has some weaknesses such as not allowing sophisticated rules that application firewalls usually do. We recommend that EFW be used as one of the protection mechanisms in a system based on the defense-in-depth concept that consists of application firewalls, intrusion detection systems and gateway protocols.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. PROBLEM STATEMENT....1
B. MOTIVATION AND OBJECTIVES....1
C. ORGANIZATION....2

II. BACKGROUND....3
A. INTRODUCTION....3
B. OVERVIEW....4
C. COMPARISION OF CONVENTIONAL AND MODERN FIREWALL SYSTEMS....5
1. Location....6
2. Recollection....6
3. Filtering Level....7
D. PROS AND CONS OF HOST-BASED FIREWALLS....9
E. THE ADVANTAGE OF CENTRAL CONTROL IN NETWORK SECURITY....10
F. SUMMARY....11

III. EMBEDDED FIREWALL SYSTEM....13
A. INTRODUCTION....13
B. OVERVIEW OF EFW....13
C. SYSTEM ARCHITECTURE....14
1. Management Console....14
2. Policy Servers....15
3. Devices....15
4. Domains....15
D. OPERATION OF SYSTEM....16
E. IPSEC OFF-LOADING....16
F. PROS AND CONS OF THE SYSTEM....17
G. SUMMARY....18

IV. RELATED WORK....19
A. INTRODUCTION....19
B. OVERVIEW....19
C. EFW'S ROLE IN DDOS ATTACKS....20
D. EMBEDDED FIREWALL DEFENSE....21
E. BENCHMARKING TERMINOLOGY FOR FIREWALL PERFORMANCE....22
F. BENCHMARKING METHODOLOGY FOR FIREWALL PERFORMANCE....23
G. SIMPLIFIED HIPAA COMPLIANCE USING EFW....24

V. EFW SYSTEM EVALUATION....25
A. TEST CONFIGURATIONS....25

B. TEST APPLICATIONS 27
C. SECURITY TESTING 29
1. Filtering Level Detection Test 29
2. Scanning Test 31
D. PERFORMANCE TESTING 32
1. Network Setup 32
2. Throughput Test 34
3. Off-loading Test 38
4. Frame Loss Test 39
5. Roaming Test 43
E. ANALYSIS 46
VI. SUMMARY 55
A. SUMMARY 55
B. FUTURE WORK 57
APPENDIX A. STATISTICS DATA 59
APPENDIX B. FIREWALL RULE SETS 75
LIST OF REFERENCES 77
INITIAL DISTRIBUTION LIST 81

LIST OF FIGURES

Figure 1. Components of EFW system 14
Figure 2. Test configuration of a dual-homed firewall 25
Figure 3. EFW firewall rule adjust window 30
Figure 4. SPF firewall rule specification window 30
Figure 5. Logical network topology used for throughput testing. 32
Figure 6. Logical network topology used for packet loss testing 33
Figure 7. Baseline throughput (KB/second) of NIC with different sizes of data. 35
Figure 8. Throughput (KB/second) of EFW when different sizes of rule sets are applied. 37
Figure 9. Throughput (KB/second) of firewall systems when IPSEC is enforced 39
Figure 10. Script flow chart 40
Figure 11. NDP values of EFW under different loads using 64 bytes ICMP packets and large size policy applied 41
Figure 12. NDP of EFW and SPF with ICMP 42
Figure 13. Maximum throughput percentage achieved before any packet loss with UDP 43
Figure 14. Baseline throughput (KB/sec) of roaming NIC 44
Figure 15. Throughput (KB/second) of roaming devices 45
Figure 16. NDP of EFW and SPF of roaming NIC with ICMP 45
Figure 17. NDP of EFW and SPF of roaming NIC with UDP 46
Figure 18. Packet loss percentage of EFW and SPF systems 49
Figure 19. OSI stack coverage of firewall systems 50
Figure 20. An example of a small-scale EFW configuration 51
Figure 21. An example of a large-scale EFW configuration 53

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. List of open ports at the EFW NIC 31
Table 2. Performance test results of EFW and SPF systems 47
Table 3. Security capabilities of firewall systems....48
Table 4. TCP throughput (KB/sec) results of NIC via TTCP....59
Table 5. TCP throughput (KB/second) with different size of rule sets applied.....60
Table 6. Throughput (KB/seconds) of firewalls with IPSEC 61
Table 7. Packet loss test results of stationary EFW using ICMP packets....62
Table 8. Packet loss test results of stationary SPF using ICMP packets 64
Table 9. Packet loss test results of stationary EFW using UDP packets 66
Table 10. Packet loss test results of stationary SPF using UDP packets 68
Table 11. Packet loss test results of roaming EFW device with ICMP packets 70
Table 12. Packet loss test results of roaming EFW device with UDP packets....72
Table 13. No drop point test results of EFW 74
Table 14. No drop point test results of SPF....74
Table 15. Small firewall rule set. 75
Table 16. Medium firewall rule set. 75
Table 17. Large firewall rule set. 75

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my sincere thanks to Dr. Wen Su for her motivation and support throughout this study. Her efforts have given me an invaluable learning experience.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Firewalls are important tools in computer system protection. A firewall is a computer system that sits between a protected network area and the rest of the network and attempts to stop malicious traffic from entering the protected network, while allowing legitimate traffic to pass in or out. In other words, firewalls are an effective security mechanism for protecting a local computer system or network of systems from network-based security threats and vulnerabilities while at the same time supporting access to the outside world.

3COM Corporation ® (3COM) Embedded Firewall System (EFW) is a newly introduced firewall system that has a solution for one of the most important limitations of firewalls, preventing insider attacks. Moving the firewall from perimeter into one more step back in defense-in-depth approach [NSA2005], the firewall functions now work on the critical point in the network, Network Interface Card (NIC). EFW works on lower network layers, unlike software based firewalls running at higher layers on the local host. By processing data at the lower layers, EFW can improve processing speed and increase performance. In addition, it is not as easy to deactivate EFW as with software based firewalls because attacker needs to have a physical access to the host computer in order to disable the NIC.

However, there has been always a trade-off between the performance and utilities of a security system. One can not expect from a particular security system to comprise all of the utilities and also have the best performance. Furthermore, estimating efficiency of a security product, such as a firewall system, is a very hard task itself and demands a great amount of knowledge, time and resources.

B. MOTIVATION AND OBJECTIVES

Although, there is not a well-defined procedure to evaluate a firewall system so as to be sure that it fulfils the security requirements of an organization or company, there are

some recent studies in order to describe the standards and provide methodology for analysis of firewalls.

Firewall providers have no doubt had done some testing on their product, prior to distribution. However, being absent from an approval whose job is only to evaluate in objective manner, these testing should not be taken as a proof of meeting the terms of a valuable firewall.

The goal of this research is to evaluate the 3COM EFW as a newly developed firewall system. The research follows the methodology and standardization offered for firewall performance analysis by RFC 2647 and RFC 3511, when applicable.

The thesis provides information on whether EFW is a usable tool in a comprehensive network defense system. Also, the thesis discusses the benefits for network security in general and specially for military networks.

C. ORGANIZATION

The main ideas of seven chapters building this thesis are as follows:

- Chapter I – Introduction: Identifies the purpose behind conducting this research, establishes the goals for thesis.
- Chapter II – Background: Provides information on firewalls and summarizes the previous studies related to EFW.
- Chapter III –Embedded Firewall System: Demonstrates basic principles behind EFW system.
- Chapter IV – Related Work: Lists previous studies specifically on EFW and firewall evaluation methods in general.
- Chapter V – EFW System Evaluation: States how the testing is done and how the result data is collected and analyzed. Presents the data collected from testing and discusses about the results.
- Chapter VI – Summary: Explains the research results and make recommendations on how to use EFW system in a defense-in-depth concept.

II. BACKGROUND

A. INTRODUCTION

The requirements for Information Security have changed radically during the last few years. The revolution started with the invention of the computer. Computers increased the need for security more electronically rather than the old style of physical and administrative security. Another change came with the ability of communication between the computers which generated the need for security of information traveling in the network between the computers, defined as network security. But such a security definition is still missing some point, security of collection of networks connected to each other, which is covered by internet security.

These categories of security may interact with each other what makes it very hard to say exactly which one is ending and the other is starting at a particular location. NIC stands in one of such a critical point that may be accepted as a boundary between these categories. NIC resides on the computer but it is starting point for networking, more significantly, it is the only point where attacking traffic can use to enter the system to be attacked.

However, attacking traffic does not necessarily enter the system from the world outside always; instead a demoralized or annoyed user in the home network, a.k.a. inside attacker, may trigger such an attack traffic emerging from inside of the protected network. Obviously, NIC is also the only point an inside attacker can exploit the vulnerabilities of home network and make the information accessible to unauthorized people. Users inside of the home network may not be generating such a harmful traffic intentionally, however recent studies show that percentage of attacks by insiders is increasing considerably.

There are two main approaches for preventing attacking in networking. One is focusing on computer security, hardening the possible vulnerabilities in Operating System (OS) or even in hardware level, also known as defense-in-depth approach. The other one is to take actions closer to network security side which consists of putting

protection efforts such as filtering and encryption into a perimeter defense concept. Firewalls have been one of the most common and simplest ways of perimeter defense techniques; they work by filtering the traffic going out or coming in. But, as the same for almost every protection mechanism, firewalls have their own limitations.

They are very efficient in preventing access to inside network if the rule set is defined convincingly. In contrast, they are not very successful at avoiding the attacks originated from inside. Moreover, during the filtering process, firewalls have to consume some resources of their host. In fact, sometimes resources are so limited that a firewall may take hold of a great proportion or even all of resources. In that case, the firewall itself becomes the bottleneck and the performance of network decreases considerably. On the other hand, sometimes there may be a number of firewalls spread into network in order to avoid firewall from becoming the bottleneck. Nevertheless, the control of more than a reasonable number of firewalls may raise a management problem at that point. More firewalls may cause a need for more concentrated communication between control unit and firewalls, which limits the scalability of the network actually.

B. OVERVIEW

During the last years, the war between the security professionals and hackers caused more efficient firewall systems to appear. In the early years, it was sufficient to have a firewall, in a perimeter defense concept, but; in this day, perimeter firewalls are no longer acceptable. Moreover, today's networks in general are no longer have clearly definable perimeters.

Modern firewalls are closer to the defense-in-depth model, which can be simply defined as "don't put all your eggs in one basket" strategy of security. Additionally, many attack attempts fail to penetrate well-configured firewalls, especially if they have a "deny everything not specifically allowed" policy.

EFW is an implementation of defense-in-depth approach indeed. It moves the firewall from software into hardware level and allows using another layer in defense

design. Moreover, it has a control and management architecture which allows the network administrators easily audit the network attacks and take required counter measures.

C. COMPARISION OF CONVENTIONAL AND MODERN FIREWALL SYSTEMS

The most important cause of changes in the firewall design was naturally what was expected from them. These expectations listed below become also the main design principles of firewalls: [Cheswick2003]

- By restricting access to the network, all data transfer should be done via firewall.
- Security policy should be carefully followed in the decision process on allowing and preventing network traffic. If more than one security policy exists, then different policies may be assigned to different firewalls.
- OS used in the system should not allow unauthorized access to the firewall.

In order to reach these goals, firewalls have used different kind of techniques to control access and enforce the site's security policy. [Smith1997] lists four of these general techniques:

- Service Control: The firewall decides on which services are allowed in the host network. The decision may be done based on the investigation of header information such as source address. Furthermore, a proxy may be set in order to interpret every service request and process.
- Direction control: The firewall determines directions to which are the services are allowed or denied. Some services are allowed in both inbound and outbound connections, some are allowed for only one way.
- User control: The firewall controls the access level for the users inside of the network. The control mechanism can also be applied to outside users by

implementing a Virtual Private Network (VPN), and using appropriate encryption mechanism such as Internet Security Protocol (IPSEC).

- Behavior control: Some of the firewalls are able to control the behaviors of the particular services as well. For example, a firewall may look at in the attachment of an e-mail in order to eliminate viruses.

The various numbers of design goals and techniques caused to come out different and inconsistent names for the various firewall systems. The classification of these approaches needs to separate these systems more structurally and functionally. Three main specifications may help to have a more generic classification: Location, storage and filtering level.

1. Location

Firewalls may be integrated into a router, switch or a NIC. Basically, a router that has Access Control Lists (ACL) configured may be considered as a firewall. These ACLs inspect various header fields against the rule set in order to make routing decisions.

Furthermore, there may be one firewall protecting whole network by standing on the gateway of the network which is known as network-based approach, or multiple firewalls may be distributed through the network, also known as host-based approach.

In the network based approach, firewall is located at the gateway of the network or subnet. The main problem of that approach is not being able to filter packets that are not leaving network, residing inside instead.

In the host based approach, each host has its own firewall. The main problem of this approach is to control the firewalls. An acceptable solution is connecting each host to a particular node in order to provide central control.

2. Recollection

Filtering is an automated way of making things easier for security of communication. However, some of the earlier firewalls were missing a basic principle of

computing which is classified as recollection. Recollection involves storing and retrieving information. [Denning2003]

Recollection can be added by including a memory into firewalls. This memory holds a table in order to keep track of connections already established. This implementation helps some of protocols such as File Transfer Protocol (FTP) to run through a firewall. FTP is a communication protocol which is using connection oriented capability of Transmission Control Protocol (TCP). By design, FTP server opens a new connection to a random port like such as 5064. After a FTP session is started, both receiving and transmitting sides keep the connection alive in order to avoid overload of connection establishment. However, if a firewall is located between these communicating sides, this firewall has to also be aware of a connection that will be active for a while. The firewalls with an ability to do recollection are defined as dynamic or stateful firewalls whereas the others are defined as static or stateless.

A dynamic or stateful firewall creates a directory for each established connection. This makes it possible to tighten rules in order to let incoming traffic to the ports that fit the profile of the entries in this directory. For FTP example above, a dynamic firewall will create an entry for the FTP server's IP and port number, which is 5064 in our case. When a packet comes from this specific IP and port number, the firewall will look at its table and discover that a connection is already established between a client in the protected network and the FTP server.

On the other side, a static or stateless firewall makes its decisions on an individual packet and does not take into consideration packets before this particular one. Firewall has to do processing in order to allow or deny every packet passing by if there is not a well defined rule for this particular packet. An FTP packet with a destination port such as 5064 will be dropped by a stateless firewall, although it is a part of a legitimate FTP session.

3. Filtering Level

Each kind of networking involves some abstraction in order to provide more modularity and reduce complexity. A standard way is to put some kind of header or

trailer to the packet when it is traveling through the layers of Open System Initiation (OSI) model. Headers may have lots of information about what is carried in payload, but sometimes it may not be enough for a firewall to decide whether the packet should be allowed to pass or not. There are methods like tunneling a packet inside of another packet that are used by attackers widely.

In the tunneling method, attacker puts the malicious code inside of an innocently looking packet. Internet Control Management Protocol (ICMP) packet tunneling is a classic example for tunneling attacks. Most of the network administrators simply allow ICMP in order to help network management. However, an attack, by using "Loki" tool easily found in the Internet, can easily be organized by sending remote control commands to a victim computer by hiding them in ICMP packets. Some of firewalls only look at the headers but not in the payload when they are performing filtering. This may leave the remote commands in ICMP packet unnoticed when it is penetrating into home network even though it should not be let passing through the firewall.

Other kind of firewalls looks deeper all the way to the payload and inspects the payload as well. For sure, this demands a greater effort of the device but this yields more intelligent filtering. Moreover, some application firewalls merge Intrusion Detection System (IDS) and firewall abilities at the same device. Firewalls with IDS capability compare the traffic patterns with known attack signatures, when filtering the arriving packets based on the ACL as well.

As a result, by using these techniques and aiming to reach the goals stated above, one can expect following capabilities from a firewall:

- A firewall supplies a single point that keeps unauthorized users out of the network, prohibits potentially vulnerable services leaving the network and provides protection for different kind of IP spoofing and routing attacks.
- A firewall provides ability to monitor the network traffic in order to audit security related events and analyze the causes of these events.

Although they are not security related, a firewall may serve as a platform for Network Address Translation (NAT) and Port Address Translation (PAT). Moreover, using tunneling method defensively this time, VPNs can be established through firewalls.

However, firewalls are a protection mechanism used in perimeter defense so far. If there are vulnerabilities and threats inside of the perimeter, firewalls basically fail. Some of these vulnerabilities are the following:

- The firewall cannot protect the attacks that bypass the firewall such as a dial-up connection made between an internal system and an Internet Service Provider (ISP).
- The firewall does not protect against an internal threat such as an employee of a company who corporate with an external attacker.
- The firewall may not be able to protect against the transfer of malicious code such as virus-infected files. Because of large variety of OSs and applications need to be supported inside the perimeter; it would be impractical for the firewall to scan everything incoming.

D. PROS AND CONS OF HOST-BASED FIREWALLS

In the host based approach, host performs the firewall function locally. The primary advantage of this approach is the ability to detect attacks that is not only traveling across the network, but also going from a computer to another one in the same network.

In a common scenario a hacker will often gain access to a web server or mail server inside the home network. Once the user privileges are obtained, the hacker will attempt to elevate his or her privileges to root or administrator level. After the desired level of access has been achieved, the intruder can place a “Trojan horse”, modify system and security logs, run packet-sniffing applications and furthermore take over other computers on the network. By preventing the exchange information between computers in the home network, host based firewalls stop the hacker from capturing more information from the network.

Even though host based approach may look more efficient than network based approach in this point, it has some limitations:

- Data processing impacts performance of the hosts.
- Every host needs a host based firewall to be installed.
- If the host is compromised, firewall process can be detected and possibly terminated.
- Maintenance of security profiles is harder and needs more resources.

In the network based approach, firewall is located on the gateway of the network. One of the advantages of this approach is to be able to see traffic that is destined for multiple hosts. Another advantage is not to have an impact on the performance of the hosts except the one hosting firewall. Additionally, management is simpler because there isn't a distributed topology as is in the host-based approach. Both processing and controlling may be done at one particular point in the network. On the other hand, network based approach have some weaknesses such as the ones listed below:

- It may loose some packets if the traffic gets heavy.
- It will not prevent host based attacks or host to host attacks that do not travel across the network link.

E. THE ADVANTAGE OF CENTRAL CONTROL IN NETWORK SECURITY

Management of host based firewall systems is more difficult than network based model especially when maintenance is considered. Many organizations do not have the resources to provide each and every employee with a dedicated station. In these environments users often share a workstation, carrying different functions with them, making it very difficult to maintain the desired security policy while providing efficient service to all users.

Moreover, although security issues in a network can be handled by each of the nodes in the network; if the number of the hosts is reasonably small, this is not true for

larger networks. Management of network security on a large network can be more difficult as network administrators have to deal with the task of setting up a number of patches and updates to various platforms periodically. Although in most of the cases the majority of the users will share common needs and applications, some of the users and groups may have special needs. Web servers, mail servers, name servers and many other hosts are example nodes that are requiring a different security profile. Centralization and automation of control may save valuable time and effort at this time.

Central control allows network administrators to regulate the behaviors of the network against different types of attacks. Administrators do not have to walk off to every host in order to configure security rules. They are able to do it from a central node in the network or even further, from outside the home network by connecting to this particular node remotely.

F. SUMMARY

Firewalls are naturally changing due to the needs emerging from newest vulnerabilities and threats discovered. One of these threats to old fashioned firewalls is the possibility of attack from insiders.

Lately developed firewall systems, such as EFW, usually have multiple components located at hosts in the network and they aim to solve insider attack problem in a defense-in-depth approach. But managing this system appears like another problem when every host has a firewall of its own. Moreover, putting all these functionalities into one security system generates the trade - off between functionality and performance.

THIS PAGE INTENTIONALLY LEFT BLANK

III. EMBEDDED FIREWALL SYSTEM

A. INTRODUCTION

Many network administrators have installed one or more firewall systems between their network and the Internet to filter traffic. These firewalls usually examine network-oriented properties of traffic, like source addresses and protocol identifiers. As observed in the Chapter II, by installing the firewall at the perimeter, the network is protected against external attacks. A well-known shortcoming of network-based firewalls is that they only protect the network from outsider's attacks.

Host-based firewalls, which are usually implemented at software layer, can address insider attack problem by placing the firewall on the individual host. The host-based firewall will block attacks regardless of whether they originate from outside or inside. However, host-based firewalls focus on solutions that were installed into the host's OS. This type of installation has the weakness that an attacker can disable the firewall if an attack on the host succeeds. EFW yields an alternative approach that incorporates advantages of both host-based and perimeter-based systems as today's modern firewall.

B. OVERVIEW OF EFW

The 3COM EFW uses a client - server based system, where the client PC installs the EFW client NIC and have the security policies on the EFW centrally controlled by a server machine.

Server side of the software allows network administrator to define a firewall rule set, through a centrally managed console and issues defined rules to the EFW cards by a Policy Server that is responsible of storing and distributing "policies" to clients. A policy in fact, is an ACL that determines what action will be taken when a typical kind of packet arrives into EFW device.

C. SYSTEM ARCHITECTURE

The EFW consists of following architectural components:

- Management console
- Policy servers
- Devices
- Domains

Figure 1 below demonstrates these components and the connection between them in one EFW domain. All computers in the figure are assumed to have an EFW NIC (Device) installed.

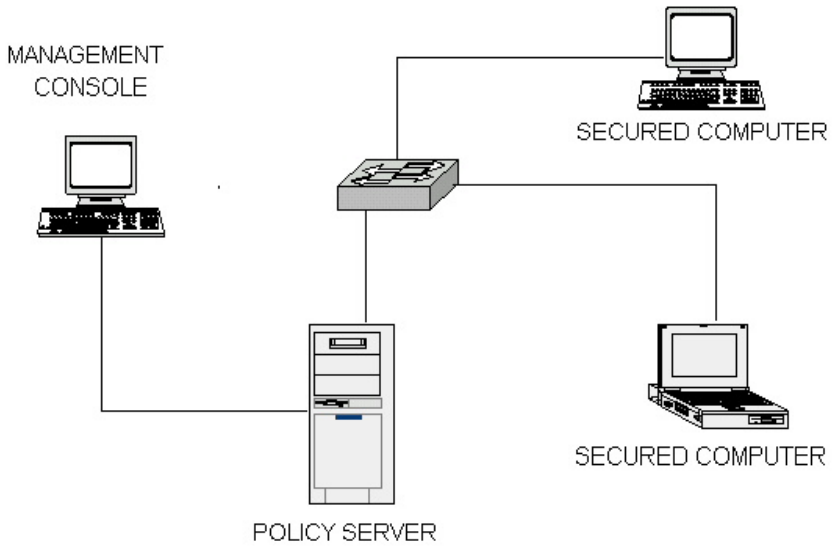

Figure 1. Components of EFW system

1. Management Console

Management Console is the administrative interface to the Policy Server. Administrators configure the system and observe the system data using the console. Management console may be on the same computer where the policy server is, or it may be on a remote host. Moreover, Microsoft ® Management Console (MMC) of Windows OS can also be used in order to access most often used functionalities of Management Console.

2. Policy Servers

The Policy Server controls EFW devices by implementing administrative orders received from Management Console. Policy Server converts high-level commands sent from Management Console into ACL rules that EFW devices can enforce during packet filtering. Furthermore, Policy Server receives and processes "heartbeat" messages from EFW devices that contain IP address and recent policy status of the devices. Also, Policy Server receives and processes audit messages coming from EFW devices. Policy Server stores the data used in policies and auditing information via a Database Management System (DBMS).

3. Devices

EFW devices filter the packets incoming and outgoing based on the ACL rules distributed by Policy Server via policies. The 3COM EFW NIC is different for servers, workstations and laptops. Mobile NIC used for laptops supports roaming feature, i.e. NIC can be used either in the protected network with a distributed policy or in another network with a pre-saved offline policy.

4. Domains

An EFW domain consists of one Policy Server and a number of EFW devices. Dividing network into multiple domains decreases the control message load in the network and ensures that only necessary messages are distributed to one particular Policy Server. Conversely, Policy Servers are responsible for distributing policies only to the clients which are in their domain.

A policy defined within an EFW domain can be assigned to any EFW device in that domain. Furthermore, audit queries can search all audit data generated within a domain.

3COM recommends not exceeding 1000 devices in a particular domain. Moreover, 3COM advises to have a back-up Policy Server for enhanced availability. There may be up to three Policy Servers in each domain including the original one. [3Com2003]

D. OPERATION OF SYSTEM

When an EFW device boots up, it connects to Policy Server in order to download the policy assigned to it. If EFW device cannot download the policy for any reason, then it goes with the policy that it used at the last time. In the case of a roaming device, the EFW device first figures out its location and then acts in the proper way based on whether it is in a EFW domain or not. If the roaming device is in an EFW domain, it follows the same step with a stationary EFW device. Otherwise, the roaming device enters a "fallback" mode and loads a pre-saved offline policy. In other words, a roaming device may have two policies, one policy for its local network and another policy for a remote network.

Stationary devices operating normally, enforcing the latest issued policy continues to do so until a "wake-up" occurs and reset the cards. Wake-up is a short message that alerts the Policy Server about a significant event that happens on the EFW device such as boot up or reset.

EFW devices periodically send "heartbeat" messages to the Policy Server. Heartbeat message is a short message informing the Policy Server that a particular EFW device is operational. If a policy distribution fails to a secured host, next heartbeat from this particular host helps the Policy Server to determine the failure in distribution and sends the policy to the host again.

EFW devices send audit messages to Policy Server. However, if Policy Server is not reachable at a moment, EFW devices do not keep audit messages. All audit messages are recorded in DBMS of Policy Server and they can be viewed via Management Console at any time.

E. IPSEC OFF-LOADING

IPSEC is a standard for securing IP communication by encrypting and authenticating IP packets. The specification of IPSEC is defined in 1998 [RFC 2401].

Internet Engineering Task Force (IETF) has an official working group studying to make IPSEC architecture a standard for IP packet traffic. As a result, IPSEC is expected to become more widely deployed.

EFW devices contain a special chip set and associated firmware to provide cryptographic acceleration for data links using the IPSEC protocol. In particular, the board of NIC contains specialized integrated circuits to provide 3-key Data Encryption System (3DES) and Secure Hash Algorithm (SHA1) integrity. IPSEC off-loading feature allows part of the encryption processing to be carried out on the NIC instead of the CPU of the host PC. The acceleration in IPSEC processing of EFW system is examined in the Chapter V.

F. PROS AND CONS OF THE SYSTEM

Management Console and Policy Server together constructs the central control mechanism of EFW. As we discussed previously, centralization helps administrators to control the behaviors of the network against different types of attacks. Interface offered by MMC makes controlling process more user-friendly. However, EFW uses a variety messages such as heartbeat messages in order to maintain this central control mechanism. A trade-off appears between performance and utilities of the EFW system.

EFW devices are actually host-based firewalls, of which pros and cons discussed in Chapter II. Different from conventional host-based firewalls, system packet filtering in EFW is done at the NIC, mostly in hardware level. Locating the firewall at NIC prevents an attack possibility based on compromising the OS running on the host. Moreover, performing filtering at NIC should increase the performance of firewall, which is examined at Chapter V.

EFW system has the ability to off-load IPSEC cryptography processing from the OS to NIC, which enhances IPSEC performance. EFW treats IPSEC like any other protocol. That is, it can permit or deny it. The performance gain of EFW from off-loading also tested in Chapter V.

G. SUMMARY

EFW is proposed as a combination of host-based and hardware firewalls that merge advantages of two firewall approaches. The architecture of EFW consists of four main components. These are Policy Server, Management Console, EFW devices and the domain that contains one or more of other components. EFW components communicate with each other to maintain consistency between server and clients.

EFW may be integrated with other systems in order to serve in a defense-in-depth approach. One of the main advantage brings EFW in front of other systems is its ability to off-load IPSEC process into EFW NIC. Certainly, EFW has a lot more advantages than that but it has some weaknesses as well.

IV. RELATED WORK

In this section, previously conducted academic studies and research of industrial organizations will be reviewed. First, we will summarize the studies directly related to the evaluation of EFW. Secondly, we will investigate published answers to the question of "how the firewall evaluation should be performed?"

A. INTRODUCTION

EFW is newly developed system so there has not been much analysis and evaluation work done to it. In fact, the concept of evaluation of security systems, including firewalls, started only a few years ago. Most of the companies do some benchmarking tests before deciding what kind of a firewall they may use for securing their network. Benchmarking involves running a number of tests and trials against different firewall systems to evaluate the relative performance.

However, when a fundamentally new system like EFW is proposed, existing benchmarking techniques becomes limited and impracticable. Benchmarking defines a set of metrics and compares their measured values to those of a system judged to be the best. However, in case of evaluation of a fundamentally novel system, metrics are not well defined yet and there is not such a best system for comparison. The evaluation method of EFW as a new firewall system should be more general, combining both theoretical ideas and practical specifications of all systems and provide a fair platform for comparison of different systems.

B. OVERVIEW

Previous studies on EFW system have already showed results regarding the basic security utilities of the newly proposed system. Students at the Naval Postgraduate School (NPS) [Burrows2004] evaluated the EFW system under simulated Denial of Service (DOS) attacks. Another study [Stewart2004] focused on the integration of EFW with other firewall systems available in order to represent a defense-in-depth portrait of

network security. Besides these academic studies, industry also carried out study on whether EFW allows more secure network structure. Secure Computing Corporation provided a mechanism to enforce privacy rules recently established under the Health Insurance Portability and Accountability Act (HIPAA) by using the EFW system [Secure2001].

There is also some standardization study for evaluation of firewall systems. A Request for Comments (RFC) issued recently offers a benchmarking methodology for firewall performance [RFC3511]. In addition, RFC 2647 gives a list of benchmarking terminology for firewall performance analysis. In this chapter, the related studies are summarized.

C. EFW'S ROLE IN DDOS ATTACKS

The Master's thesis work titled "Evaluation of Embedded Firewall System and Its Role in Protection against Distributed Denial of Service (DDOS) Attacks" [Burrows2004] tested several security features offered by EFW that help protecting against variety of attack types. EFW pre-defined policies, such as "No Sniffing", that help network administrators to create more detailed policy configurations were validated in this thesis work. Ethereal Network Protocol Analyzer (ENPA) was installed onto one client and placed into a policy that permitted packet sniffing. While the ENPA was running, the security policy for this particular client was changed so that it no longer was authorized to act promiscuously. The policy change was successful and the client was no more able to operate in promiscuous mode despite running the same ENPA process.

The thesis also discussed ways to map various policies of Information Control (INFOCON), the comprehensive defense posture and response based plans that used by Department of Defense (DOD), to the EFW client policy set. EFW provides a convenient way to enforce and change the security postures on individual client based on INFOCON levels. In addition, the thesis found vulnerability in the audit mechanism of EFW. Although EFW is capable of preventing IP address spoofing, it cannot prevent attacker from spoofing the MAC address on the client. Since some of the OS like Windows 2000 and Windows XP allow a user to change the MAC address of a NIC, an attacker can use

this feature in order to spoof his/her identity. EFW system uses MAC address as the unique key for storing audit records sent from clients at the policy server. But, policy server only checks MAC address when client is first registered to server and relies on solely on the IP addresses for policy updates. This means that a client with a spoofed MAC address will continue to receive policy updates, but it will never be able to send audit messages to the server until its MAC address is reset to the same MAC address at the time of the card's registration.

The thesis also carried out performance evaluation and concluded that EFW offered some very practical security advantages such as ability to centralize security control while maintaining host-based packet filtering processing. However, the weaknesses of the EFW system include limited protection from Distributed Denial of Services (DDOS) attacks, limited auditing, and poor throughput performance compared to regular NICs.

D. EMBEDDED FIREWALL DEFENSE

The study from United States Military Academy (USMA) [Stewart2004] focused the use of NICs with embedded firewalls to supplement the security provided network-based firewalls. By using EFW in combination with other firewalls, the study showed that fighting against infections in an internal network is possible. Moreover, combining multiple firewall systems let administrators to enforce policies to computers, relieve the users of responsibility for managing their firewall and maintain central control over firewall rules.

The study also suggested an evaluation in order to test effectiveness of EFW NIC by building a small network consisting at least one Policy Server and one exploitable client. The first part in the suggested evaluation is to test some of the basic functionality of the Policy Server and its ability to create and distribute rules. The second part tests the ability of the embedded firewalls to fight against an infection on the internal network.

The evaluation classifies four different results that EFW may have for a typical attack. These results are summarized below.

- Causes no impact: The policy server cannot prevent attack.
- Mitigates the effects: A firewall rule can be created that can mitigate some of the effects of attack.
- Prevents propagation: A firewall rule can be created that halts the spread of an infection.
- Causes the attack to fail: A firewall rule can be created that prevents the attack from starting.

The study concluded that although current EFW implementations do not have a special NIC for every type of network connections, for example, there is not a wireless EFW NIC at the moment, a significant number of computer systems can still be protected. This will safeguard a large portion of today's networks while fighting against the infection in the rest.

E. BENCHMARKING TERMINOLOGY FOR FIREWALL PERFORMANCE

RFC 2647, titled "Benchmarking Terminology for Firewall Performance", defines terms used in measuring the performance of firewalls. The primary metrics used in the document are *forwarding rate* and *connection-oriented measurements*.

Forwarding rate is defined as "The number of bits per second of allowed traffic a DUT/SUT[1] can be observed to transmit to the correct destination interface(s) in response to a specified offered load". Connection is defined as "A state in which two hosts, or a host and the DUT/SUT, agree to exchange data using a known protocol". TCP is given as the main example protocol that can be used in a connection.

RFC2647 does not provide a definition for throughput but defines "goodput" as "The number of bits per unit of time forwarded to the correct destination interface of the DUT/SUT, minus any bits lost or retransmitted." The measurements in this research does not separate bits as good or bad, since all of the packets generated are measured in the tests. Therefore, instead of the term "goodput", a more general term "throughput" is used.

[1] Device under Test (DUT) and System under Test (SUT) are defined in RFC 2285. They are basically device(s) which stimulus is offered and response measured.

Furthermore, since EFW is not a network-based firewall, and network traffic does not go through EFW to another system but directly to the host computer itself through the PCI bus attached to the EFW NIC, it is not possible to measure the rate of bits forwarded to a correct destination as defined in RFC 2647. Therefore, using a similar model, forwarding rate measurements are done by directing bits back to the sender, and TCP is used in a connection oriented scheme to find the forwarding rate of EFW devices.

F. BENCHMARKING METHODOLOGY FOR FIREWALL PERFORMANCE

RFC3511, titled "Benchmarking Methodology for Firewall Performance", discusses and defines a number of tests that may be used to describe the performance characteristics of firewalls. In addition to defining the tests, the document also describes specific formats for reporting the results of the tests.

Test configurations defined in the document is separated into two kinds of firewalls which have dual-homed and tri-homed configurations. Dual-homed firewalls are generally configured to be placed at a location that connects two network areas. One set of interfaces is attached to the protected network area, whereas the other interfaces are attached to the unprotected areas. Tri-homed configurations employ a third segment called a Demilitarized Zone (DMZ) in addition to the protected and unprotected areas.

The document states a number of parameters that should be considered during the firewall testing. The tests defined in this document are listed below:

- IP throughput
- Concurrent TCP connection capacity
- Maximum TCP connection establishment rate
- Maximum TCP connection tear down rate
- Denial of service handling
- Hypertext Transfer Protocol (HTTP) transfer rate
- Maximum HTTP transaction rate

- Illegal traffic handling
- IP fragmentation handling
- Latency

The main interest of RFC 3511 is performance measurement. The document does not discuss security issues. Previous work [Burrows2004] performed "Denial of service handling" tests and showed that EFW can use only 1.95% of network utilization without dropping a single packet and EFW drops 99.03% of packets when network utilization reaches 90%. In this research, IP throughput and maximum TCP transaction rate tests are conducted. TCP transaction rate is selected instead of HTTP, as suggested in RFC3511, because EFW runs at lower layers of Open Source Initiative (OSI) stack and measuring lower layer protocol makes the results more realistic.

G. SIMPLIFIED HIPAA COMPLIANCE USING EFW

Secure Computing Corporation (SCC) carried out a study on using EFW to enforce privacy rules recently established under the HIPAA. [Secure2001] The new privacy rules are intended to reduce the risk of an individual's private health information being used in an inappropriate manner without person's permission. The rules basically require health care organizations to restrict access to personal health information in accordance with employee's roles and duties within the organization.

The experiment shows that EFW system helps to enforce such restrictions by controlling data sharing between servers and clients in the organization network. The centralized management helps the organizations to respond to changes in privacy regulations and in organization's network environment.

SCC mainly concentrates on the conceptual side of the EFW as a system that can be applied into a real world security problem. The study does not discuss about performance issues.

V. EFW SYSTEM EVALUATION

A. TEST CONFIGURATIONS

Firewalls are generally configured to be placed at a location that connects two network areas. One set of firewall interfaces is attached to the protected network area, whereas the other interfaces are attached to the unprotected network area. To a firewall, the protected areas are where the host network computers are; whereas the unprotected areas are anything located outside the host network that network administrator may have little or no control. Firewalls configured with two network areas are called "dual-homed" firewalls.

As we discussed at Chapter IV Section F, there is another configuration, "tri-homed" configuration, in which firewalls have a third area, DMZ, for adding more security by restricting access of some servers from unprotected network. Test configurations may be different based on the dual-homed or tri-homed firewall configurations. [RFC 3511] In this research, the experiments are set up in a dual-homed configuration. Figure 2 shows the basic test configuration of a dual-homed firewall.

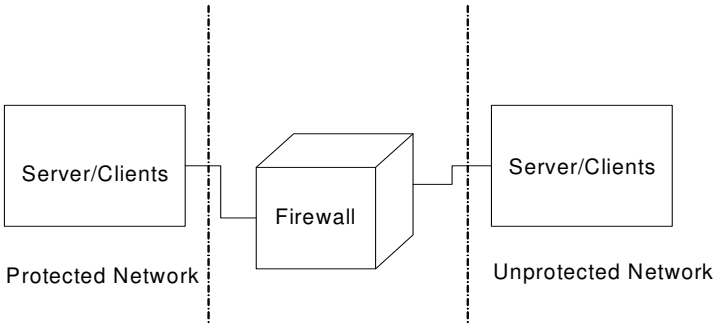

Figure 2. Test configuration of a dual-homed firewall

Firewall testing may involve a number of components in the protected and unprotected network areas, as well as inside the firewall system itself. For this research, the "black box" test approach is used as the testing method. Black box testing is a software engineering testing method that checks the outputs of a software program for given inputs in order to conform to the functional specification of the software. The inner workings of the software itself are not examined; therefore we kept the term "black box."

The reason that black box testing is appropriate for this work is that the system under test, i.e. the 3COM EFW, is a commercial product, that the inner working of the system is proprietary and is not accessible to the researchers. 3COM does not issue any detailed documentation about system components nor the source code of the system software.

EFW system is a combination of management software and firewall card hardware that allows configuring centrally managed security policies. The EFW management software is called the Policy Server. The Policy Server allows administrators to control security policies on the EFW clients. The distributed firewall component NIC is built on Peripheral Component Interconnect (PCI) technology and yields a throughput of 133 megabytes per second. The distributed clients and the server are connected via the EFW NIC, which also carries out the filtering and auditing tasks.

In this research, the basic test network environment includes a System under Test (SUT), which is a real EFW system, and emulates the protected and unprotected sides. Necessary applications are loaded on workstations and servers in order to evaluate the EFW system efficiency.

Firewall testing may be separated to two main categories: performance tests and security tests. Performance tests are related to hardware aspects of firewall and involve more quantitative data, whereas security tests simply consist of qualitative data such as determining whether the firewall is able to prevent a specific type of attack. When it comes to measuring performance of network and computer systems, different metrics are used based on the functions of the systems. For example, for a web site, the number of simultaneous users that it can handle plays an important role in performance analysis. For a firewall, the maximum bit forwarding rate that it can forward is a good way of

describing performance. Choosing the right load to apply will ensure that SUT gets assessed in the proper way and the test results matter for the system. Possible quantitative metrics and protocols that can be used for qualifying the performance of a firewall are listed as in RFC 3511. This list can be found in the Chapter IV Section F. However, one should not ignore that testing a firewall requires assessment with a selection of different protocols. Because protocols have different behaviors and firewalls react to each in different ways, a full picture of firewall performance cannot rely on the information gained from just a single protocol.

Evaluating the security of a firewall is more complicated than performance analysis because security metrics are harder to define than performance. Performance metrics can be measured quantitatively but security metrics are mostly qualitative. Security parameters are generally not only derived from the architecture, but also from ability to prevent an increasing group of sophisticated attacks. Furthermore, performance and security issues are inter-related. For example, some form of attacks can basically decrease the performance of the firewall, making the firewall the "bottleneck" of the data flow. A compromised firewall can severely degrade the performance of a network.

B. TEST APPLICATIONS

In this section, the software used in the experiment will be discussed. They can be divided into three categories, OS software, EFW software and the testing software.

Currently only Windows based OSs work with EFW. They are Windows 98, Windows 2000, Windows NT, and Windows XP. Windows XP Professional Service Pack 1, the latest issued one among the others, is installed on all clients and the server for tests in this thesis.

Only the server needs to run the EFW Policy Server software. The Policy Server and the Management Console can be run on separate hosts, but for our experiments, they are installed on the same server in order to decrease network complexity. MMC, Windows GUI driven management console, is used for accessing the Management Console.

TTCP, a network performance analysis tool, is installed on the both workstations. It measures the throughput performance between networked components. There are a number of different versions of TTCP available. Most of the TTCP versions are written for UNIX. The version used in this research is re-designed by Gregg G. Seipp from North Carolina State University and runs on the Windows platforms. [Geigg2004] During the measurements, one of workstation is used as the transmitter and the other as the receiver. TTCP can be configured to send TCP or UDP packets between the transceiver and receiver, and it measures the throughput and response time observed over the link.

NMAP, a commonly used network scanning tool, is also installed to the transceiver host, so as to find the ports that are open in the receiver side of the testing configuration. NMAP sends ICMP, UDP and TCP packets to a specific address or a range of address and gives information about the host residing on the address. The information provided includes the ports open or filtered and probable OS running on the host.

The Spirent Smartbits packet generator is used for packet loss testing in this thesis. The packet generator is controlled via a TCL script [Spirent2001] provided by Spirent Communications. This script enables the NIC installed at the packet generator to send ICMP echo messages to the client and waits for ICMP reply messages. During the testing, the TCL script calculates the percentage of the replies compared to packets sent under different load conditions. The TCL script can also be configured to use UDP packets, instead of ICMP packets, for packet loss testing. In that case, in order to echo back the UDP packets to the packet generator, the receiver runs a program that will forward the UDP packets back to the packet generator.

There are a couple of host-based firewall applications that has the ability to do packet-filtering. Among these programs are Zone Alarm by Zone Labs and Symantec Personal Firewall (SPF) by Symantec Cooperation. Host based firewall applications like SPF often asks the user when a service attempting to use a given port is allowed to do so or not. By using the answers, application sets up a base line of operations and makes persistent rules for future occurrences. A user can define system-wide firewall rules that will affect every service's network access. SPF has a built-in attack signature list and acts

like a simple IDS based on this list. The signature list is upgradeable in order to address latest threats.

C. SECURITY TESTING

EFW has a number of default defined rules that may be included into the policy enforced in the network. Examples of these built-in policy rules are preventing attacks like IP Spoofing and TCP SYN attacks. IP spoofing is controlled by disallowing a source address that differs from the address of the local interface. TCP SYN flood is handled by denying TCP connections that initiate the SYN without sending the final ACK, needed to start data transfer.

1. Filtering Level Detection Test

An important feature of a firewall is the network layer at which they can perform the filtering. We confirmed that EFW does filtering at transport layer. The policy server allows creating such rules as allow all TCP traffic and deny a specific UDP traffic from a particular host. However, we are not able to confirm that EFW does further filtering, i.e. filtering beyond IP and TCP/UDP layer. For example, EFW does not allow network administrator to define exactly what type of ICMP messages are allowed to pass through the firewall. All the ICMP traffic inbound or outbound can be denied by simply adding a rule, but there is no option to restrict specifically ICMP Route Redirect messages for example. (See Figure 3)

Examination on higher layers usually decreases the performance but adds more security capability to the system. This is probably the reason behind the decision of the EFW developers for not adding a feature to EFW for examining payload of ICMP packets. However, since ICMP messages are commonly exploited by hackers, we believe that examining at least the ICMP packet payload is worth the cost.

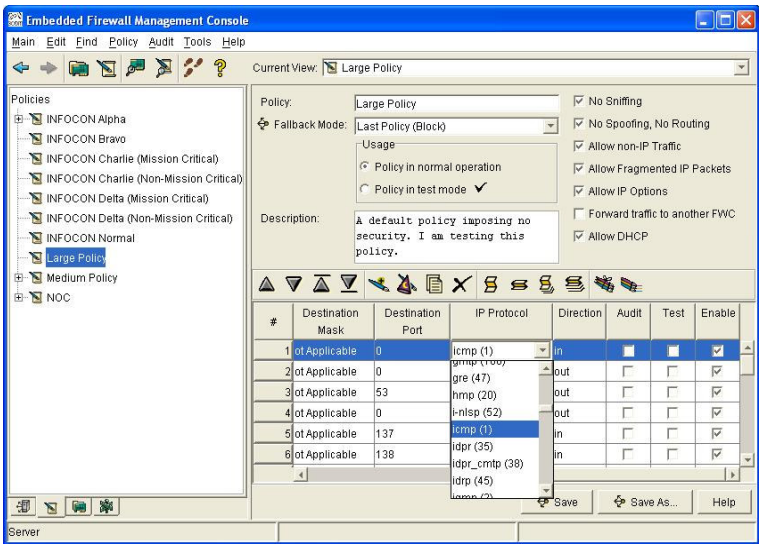

Figure 3. EFW firewall rule adjust window

In contrast to EFW, SPF is able to specify a rule for denying only ICMP Route Redirect messages, although it can allow the other kind of ICMP messages to pass through the gateway. This helps to prevent an attacker to perform a “man-in-the-middle” attack by taking over one of the gateways inside the network. Figure 4 shows the window in SPF that is used for specifying firewall rules consisting of different ICMP commands.

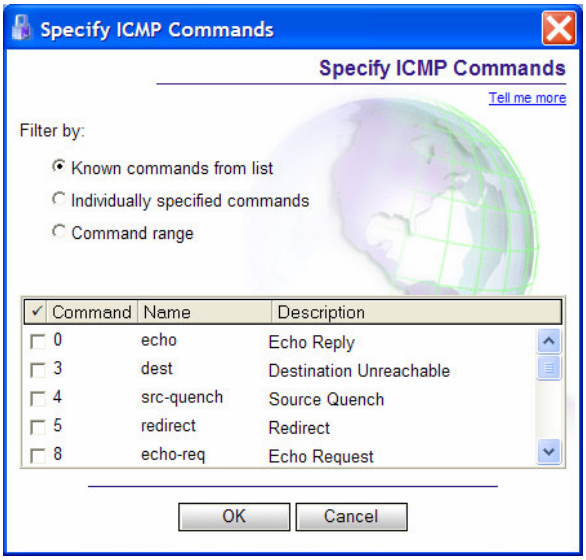

Figure 4. SPF firewall rule specification window

2. Scanning Test

NMAP, a common network scanning tool, is used to test if firewalls are capable of preventing TCP SYN attacks. NMAP sends a TCP SYN packet to all ports and waits for response in order to map out firewall's rule set. If a TCP RST comes back from one of these ports, this port is supposed to be unfiltered by firewall. If the port is filtered, then nothing should come back. Our test showed that both EFW and SPF prevented TCP SYN flood or TCP SYN scanning by checking SYN flags in TCP header, which is done through higher level filtering rather than simple IP layer filtering. But surprisingly, EFW is not able to prevent a TCP ACK packet used for scanning that looks like a reply to a request from an internal host. SPF on the other hand, by keeping track of the TCP connections, is able to discard the packets that are not related to any connection previously established. Table 1 below shows the list of the ports that are open and filtered at the EFW client after a scanning by using NMAP.

PORT	**STATE**	**SERVICE**
135/tcp	Open	msrpc
139/tcp	Open	Netbios-ssn
445/tcp	Open	Microsoft-ds
1025/tcp	Open	NFS-or-IIS
1723/tcp	Open	Pptp
5000/tcp	Open	UPnP

Table 1. List of open ports at the EFW NIC

D. PERFORMANCE TESTING

1. Network Setup

The components used in this evaluation include EFW clients, an EFW server, and the physical connections. Two PC workstations are used to emulate client system activities of a typical network. All client PCs are installed with Pentium IV CPU at 2.4 GHz or above and 256 MB of RAM. Additionally, a PC with Pentium IV CPU at 3 GHz and 1GB of RAM is used as the server. It is attached to the Local Area Network (LAN) and running the 3COM EFW Policy Server software.

The workstations for clients and the server are pre-installed with on-board Intel PRO/100 VE model NIC (Intel NIC). In addition, 3COM 3CRFW200 and 3CRFW300 model firewall NIC (3COM NIC) are installed on the clients and the server respectively, as required by the EFW setup. Since firewall cards are specially designed for EFW system, and they have some specific communication methods and adjustments; Intel NICs are used to provide the baseline value to evaluate the 3COM NIC performance. They are also used when running application firewall on the host computer in the performance evaluation testing.

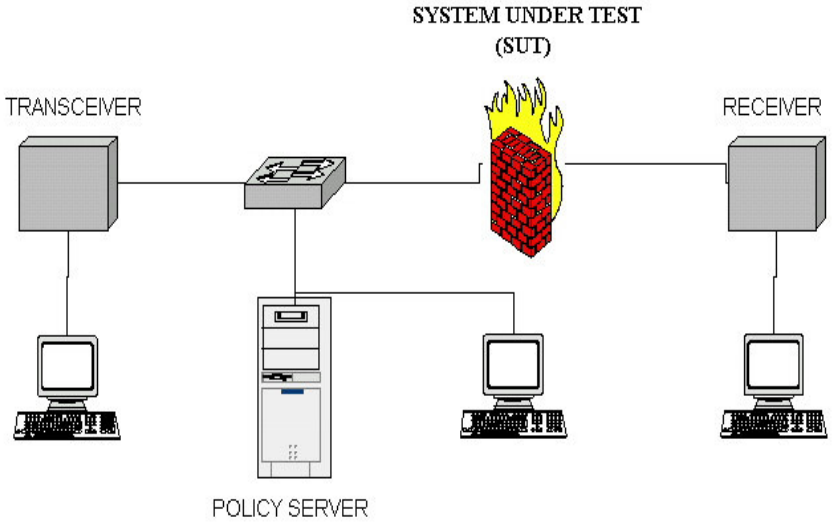

Figure 5. Logical network topology used for throughput testing.

Figure 5 illustrates the selected physical topology used to conduct throughput measurement experimentation on the EFW clients. Two clients are connected via Category 5 cable to a 4 port 10/100/1000 megabit layer-2 switch, which in turn is also connected to the policy server. One client acts as the transmitter and the other as the receiver. The throughput is measured between these two clients.

The Spirent Smartbits packet generator is also used in our experiment to measure packet loss. The packet generator has 10/100/1000 Mbps Ethernet connection [Spirent2003] and is controlled by the same server machine on which the 3COM policy server is installed. The packet generator is connected to the server and one of the clients using separate Ethernet connections to avoid intervention of control signals with test results. As illustrated in Figure 6, the server is directly connected to the packet generator via a Category 5 cable, and one of the clients is through an Ethernet switch. The control signals of the packet generator are transferred via the direct connection between the packet generator and the TCL script running on the server.

The idea behind isolating the connections between packet generator-policy server and policy server-client is to separate the EFW and packet generator system messaging. This setup provides a more real world-like environment, where EFW will have the same message overload between Policy Server and clients, and there is no packet generator and messages between packet generator and the server in the network.

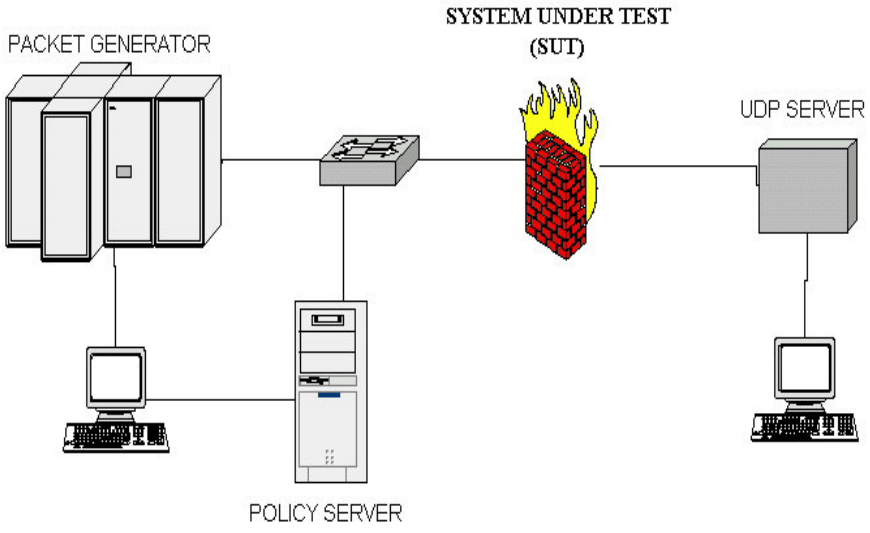

Figure 6. Logical network topology used for packet loss testing

The throughput and packet loss tests are repeated on laptops using an EFW PC card as well. The other components and the topology remain the same during testing PC cards as the topology used in testing PCI driven EFW cards.

As explained in Chapter IV Section C, some measurements are taken for EFW previously [Burrows2004]. The previous work was only based on performance and capabilities of EFW system but did not have any comparison with existing firewall systems. In this research, measurements are extended in order to provide a platform for comparing EFW with common host-based firewall systems.

For the performance testing part in this research, EFW is compared with firewall applications that have the ability to do packet-filtering. TTCP is used for measuring the delay and transmission rate. Since the NIC and firewall setup changes in the test while network topology remains the same, TTCP measures the impact of changing the firewall system on throughput. The application firewall used in the test for performance comparison is the SPF. Later on in the analysis we also use the term SPF to reference application firewalls in general.

For the performance phase of testing, we use various workloads on the network to compare the throughput of EFW and SPF. A compatible baseline performance value, measured when no firewall filtering rule is used, is found in order to determine the base configuration for comparative testing.

2. Throughput Test

Each client computer has two different kinds of NIC. One is the 3COM 3CRFW200 model used in EFW system and the other is either an Intel PRO 100/VE or 3COM 3C920. The throughput performance of a NIC is partially determined by the circuit design and quality of semi-conductor and conductors inside. Our goal is to find the experimental setting where similar throughput performance is achieved when no firewall function is applied, and use this setting to compare the impact of various firewalls on performance. Therefore, measurements are taken when no ACL is applied to the firewall systems. This is done by disabling the application firewall and disassociating EFW NIC with the Policy Server during the test. The throughput is measured by transferring data of

different size in fixed-length TCP packets using TTCP for each of the NIC and the results are shown in Figure 7. The raw data for this and further experiments may be found at Appendix A.

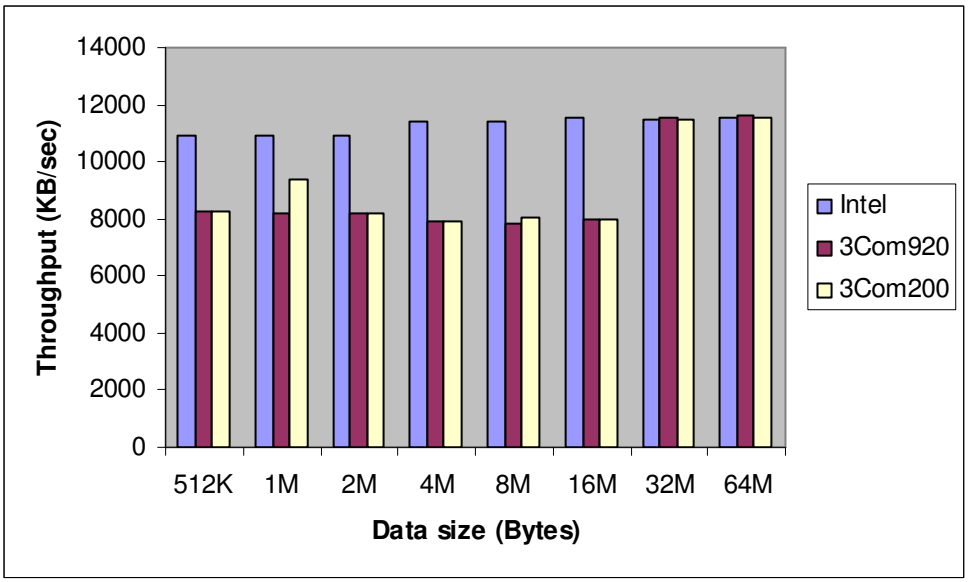

Figure 7. Baseline throughput (KB/second) of NIC with different sizes of data.

Figure 7 shows the throughput of various NICs when different sized data are transferred. The size of the data transferred using TTCP is calculated by multiplying buffer size and the number of buffers sent. The buffer size affects the throughput value much more than the number of buffers. That's why we kept the default value of 2048 as the constant number of buffers and changed the buffer size during the experiments. The results show that when smaller sized data are transferred, 3COM NIC products do not achieve as high a throughput as the integrated Intel NIC. Burrows and Lemott also conducted similar TCP testing for 3COM 3CRFW200 NIC and measured TCP throughput by sending a file with the default buffer length of 8 KB. [Burrows2004] Although they used PCATTCP, another version of TTCP, the results were exactly the same for two studies at 8 KB buffer size. In this test, all NIC reached to maximum throughput value 11.5 megabytes per second which is equal to 92 megabits per second when the buffer length is 16384 bytes (16 KB), shown as 32MB data size (16KB*2048) in Figure 7. The result is reasonable since the CAT-5 cable used in the test limits the

maximum date rate of the system to 100 megabits per second. The buffer length of 16 KB and 2048 number of buffers is used in the further testing.

Burrows and Lemott measured throughput of EFW NIC with constant buffer length in the previous study [Burrows2004], and they only turned the firewall on and off by assigning a policy to NIC from Policy Server or removing the association between the NIC and the Policy Server. However, they didn't measure the firewall's rule processing affect on the total performance of the system and they didn't compare EFW system with other type of firewall systems. In the next step of testing, we set a platform for comparing the throughput of SPF and EFW by using TTCP, and we apply three different sizes of rule sets in order to see the performance under different loads, because processing rules and the associated action may alter the performance of the firewall.

Three different policies are created at the policy server of EFW system: Large size policy, medium size policy and small size policy. The rule sets for each set of policy can be found in Appendix B. Large size policy consists of 29 rules and default rules such as "No IP Spoofing" and "No sniffing" which are already defined in EFW system. Medium size policy has only the allow rules that are required for testing by using TCP. All the other communication is denied by a general deny rule. However, as mentioned Section B, EFW does not give the opportunity to control higher level messages like "ICMP echo" or "ICMP reply", for that reason all ICMP messages are allowed. EFW does not allow deactivating all rules at a particular time. At least one default rule for denying or allowing any type of connection is needed in every policy created. Therefore the small size policy has just a general allow rule, which can be assumed as the firewall does not have any rule at all. But, it should not be ignored that firewall is still spending time accessing data even though it is not making too much decisions at this time.

Firewalls running on application layer are able to monitor OS behaviors and detect which application is trying to reach network. Since SPF is a firewall that is able to work on application level, more care is given in defining the rule set in order to keep the comparison fair. The same policies are applied to SPF by using the "system-wide settings" feature. The rules defined in this area are applied to all applications accessing to network and all data coming from the network as it is in the EFW system. Although SPF

gives opportunity to define rules specific to applications and protocols such as ICMP, these rules are disabled in the test.

As EFW is using 3COM NIC for performing firewall tasks, and this NIC has specifications special to EFW system such as sending heartbeat data in a period of time to keep in touch with policy server, the data is sent through Intel NIC when SPF performance is measured. Since previous test shows that when TTCP sends 16KB of buffer size, the throughput of the Intel and 3COM NIC are compatible, 16KB of buffer size is transferred in TCP packets by using TTCP application in the EFW and SPF comparative testing.

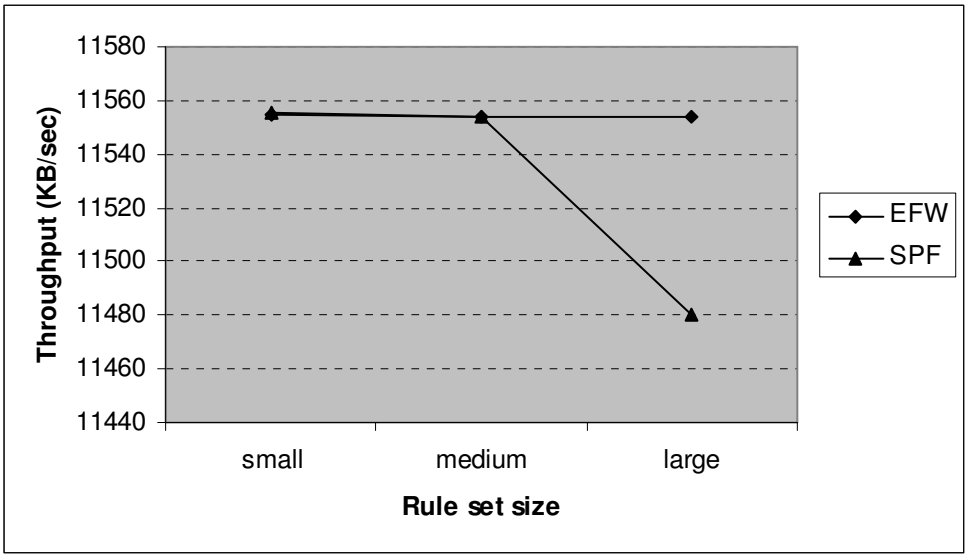

Figure 8. Throughput (KB/second) of EFW when different sizes of rule sets are applied.

Table 4 in Appendix A shows the throughput results taken from the tests. Figure 8 summarizes the results. It shows the average throughputs measured when different sized rule sets are applied. The result indicates that EFW performance is not affected very much by the size of policy rules. Maximum standard deviation is in small rule set size and it is as low as 0.96 KB/second. In fact, when the same rule sets are applied to SPF, the performance is very similar to those above except that SPF's performance results

have more variation. This implies that for the size of the rule set we chose, the size variation does not affect firewall performance with today's powerful computing resources.

3. Off-loading Test

To perform packet filtering, firewalls must examine each packet; classify the packet based on the rule set, and carry out the actions defined by the rule set. This can be a very computational intensive task for the processor depending on the rule set and the amount of traffic.

A more expensive computation task is cryptographic process. Encryption and decryption of the packets takes a lot of system resources. IPSEC is a cryptographic protocol for securing IP packets at networking layer. A firewall has to encrypt every IPSEC packet before examining it. EFW NICs has an embedded CPU for decrypting IPSEC packets. 3COM claims that EFW off-loading mechanism to take the cryptographic load of IPSEC protocol away from the host computer CPU and decrypt the packet before it ever reaches the upper level of software firewall mechanism. [3Com2004]

For testing part of the EFW performance when IPSEC is enforced, MMC feature of Windows XP Professional is used to set IPSEC connection between two workstations. 3DES and SHA1 algorithms are selected for encryption and integrity respectively. Both transceiver and receiver side save a pre-shared secure key for authentication.

TTCP application is used to obtain throughput measurements. The same buffer length of 16KB that used in baseline throughput test is used for off-loading test. Table 6 in Appendix A and Figure 9 below shows the throughput data collected from both firewall systems. The bars on the left part of the diagram that are labeled "w/IPSEC" demonstrates the previous throughput measurements whereas the bars on the right shows the throughput of EFW and SPF systems when IPSEC is enforced as the encryption mechanism in the connection between TTCP transceiver and receiver.

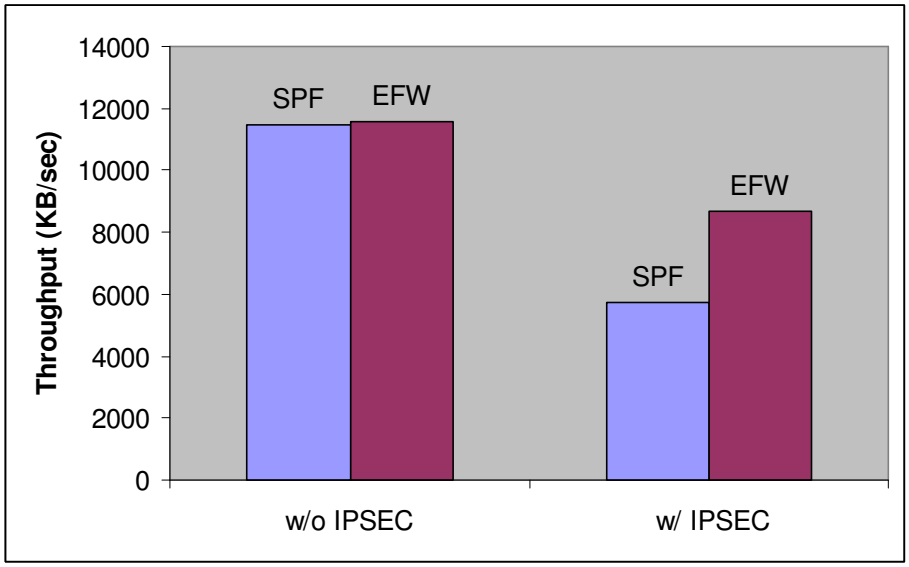

Figure 9. Throughput (KB/second) of firewall systems when IPSEC is enforced.

Results in Figure 9 show that EFW is able to get 75.31% of the throughput when IPSEC is enforced, where SPF is able to get 50.05% only. EFW off load mechanism helps to get approximately 25% more of throughput by taking the encryption and decryption work from CPU located at host to the CPU embedded on the NIC.

4. Frame Loss Test

In addition to measuring the maximum throughput a firewall system can sustain, frame loss tests are also carried out to determine at what load the NIC processing can become a bottleneck and cause frame loss. The frame loss may occur because of different reasons. The most common reasons are listed below:

- Congestion in the network
- Latency during packet transmission
- Out of sequence packets
- Frame errors

For frame loss analysis, Smartbits packet generator is connected to the layer-2 switch and ICMP echo packets are sent to the EFW client. Based on the ICMP reply packets returned from the client, the percentage of packet loss is calculated with different

traffic loads. In our test, out of sequence packets are not expected since we are not using any routing, i.e. all packets have to go through the same switch. Congestion may be occurring when ICMP echo and reply messages collide. Latency and frame errors are the most probable reasons for frame loss in our case, and these two parameters directly affect the performance of firewalls. Testing is conducted by using a script written in TCL provided by Spirent Communications. [Spirent2001] The script runs in 3 phases including sample iteration, transmitting flows and analyze data for calculating No Drop Point (NDP), which gives us the maximum throughput percentage achieved before any frame loss occur. A larger NDP indicates a more desirable firewall performance. Figure 10 below shows the script flow chart used in the frame loss analysis.

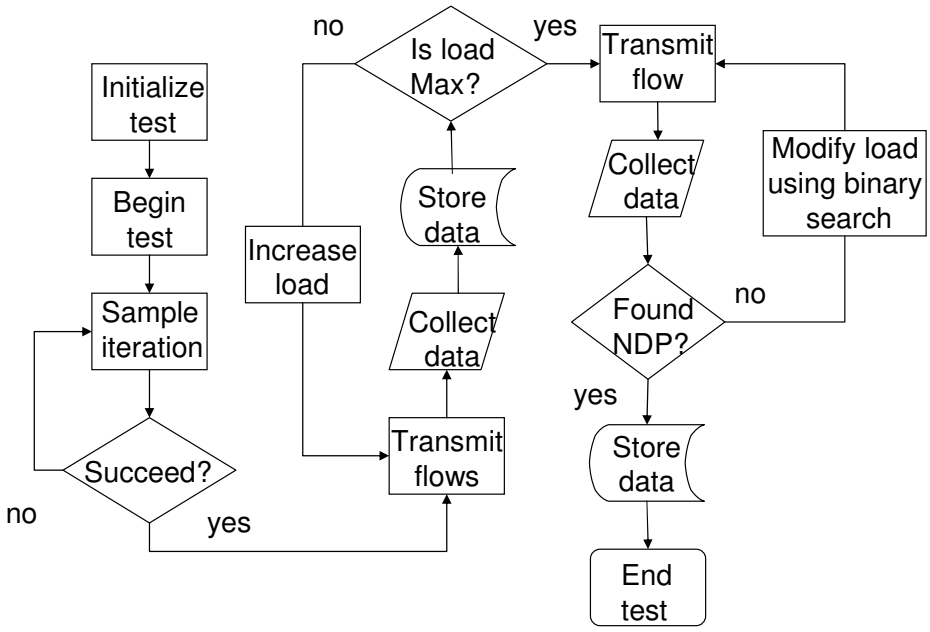

Figure 10. Script flow chart

In the sample iteration phase of the test (see Figure 11), regular ICMP packets are sent to check if the client will replay correctly. In the next iteration, Cyclic Redundancy Check (CRC) error is added into the ICMP packets to test if the client will drop the

packets. Finally, undersize and oversize packets are sent to check the correctness of the clients reply. Results indicate that EFW NIC is dropping all faulty packets including over sized ones.

When the sample iteration is finished, packet generator started to transmit packets in form of a flow. Utilization in the network (i.e. percentage of the bandwidth used) is started at 10% and is increased by 10 percent for each iteration. The percentage of the packets received is calculated, and this value is called *throughput* in the frame loss test result. The packet size is changed between 64, 128 and 1024 bytes and different policies applied with different rule set sizes while these measurements are taken. Similar to data size in the throughput test done with TCP packets, rule set size didn't affect the results much. However, the packet size has more influence on the results. Figure 11 shows the maximum throughput percentages achieved for EFW system in sample iteration phase for 64 bytes packet size and large size policy applied.

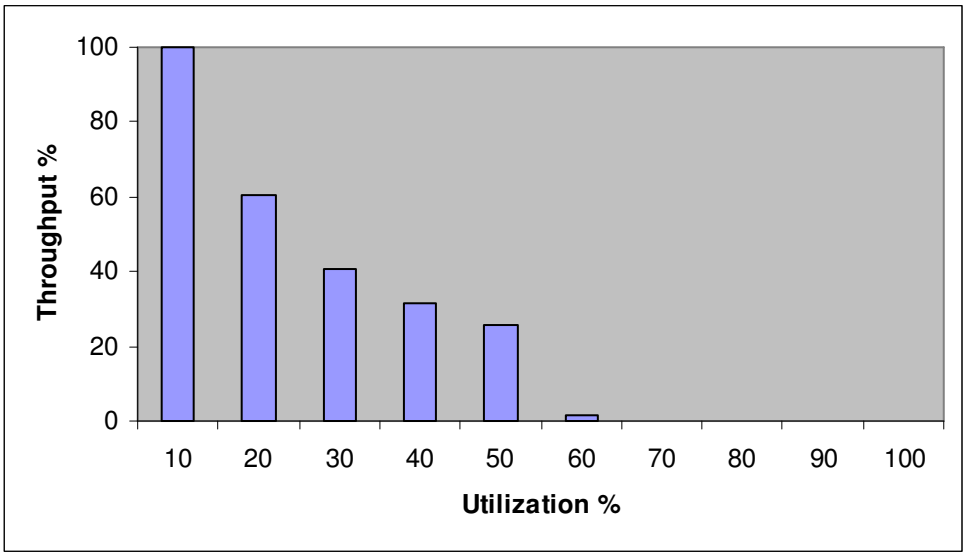

Figure 11. NDP values of EFW under different loads using 64 bytes ICMP packets and large size policy applied

The results demonstrate that EFW starts to loss packets after 10% utilization is reached. To find the NDP, the exact point at which the system starts to experience packet loss, the TCL script performs a binary search. When all packets are successfully transferred, it is assumed that test is passed and the network load is increased; otherwise,

the load is decreased. If the difference between previous and current network load (delta) is less than 0.2 percent, the test is ended, and network load value (measured in percentage of bandwidth utilization) is recorded as the NDP.

In the test, the exact NDP value found is 11.71% for EFW system. The same test phases are also applied to SPF system, with the same packet sizes. Figure 12 shows the calculated NDP of EFW and SPF systems with different ICMP packet sizes. The data collected may be found at the Table 7 and 8 in Appendix A.

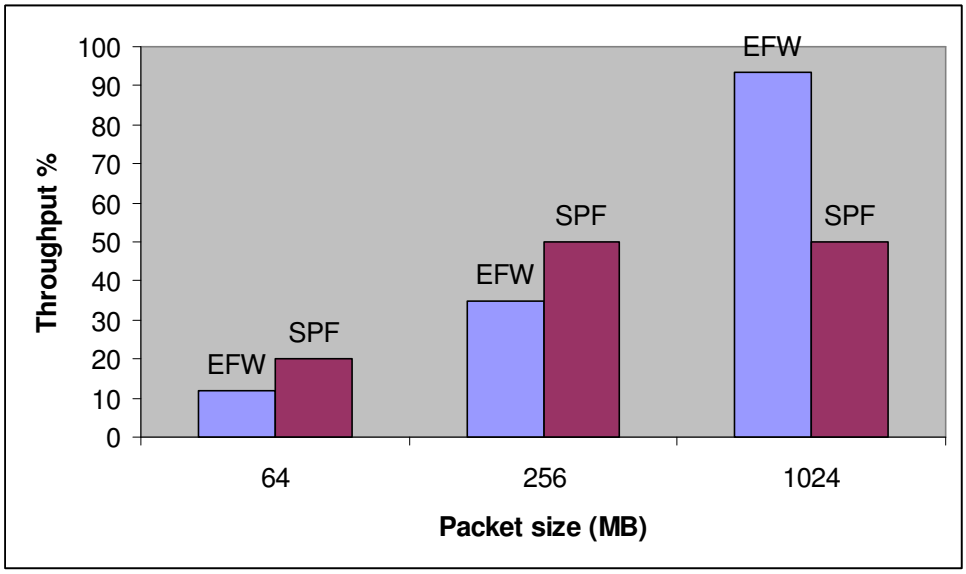

Figure 12. NDP of EFW and SPF with ICMP

Results in Figure 12 shows that SPF has larger NDP than EFW in smaller packet sizes. However, as the packet size increases EFW gains more portion of available bandwidth.

Since there is a possibility that some of NIC may not response every ICMP echo request after a limit is exceeded [Spirent2001], packet loss test is executed with UDP as well. A UDP server is set up at the EFW client with the purpose of sending back the UDP packets back to packet generator. The results show that EFW NIC is probably limiting the responses to ICMP echo requests indeed because its packet loss rate is much less with UDP compared to ICMP. Figure 13 illustrates the results achieved by UDP packet loss test.

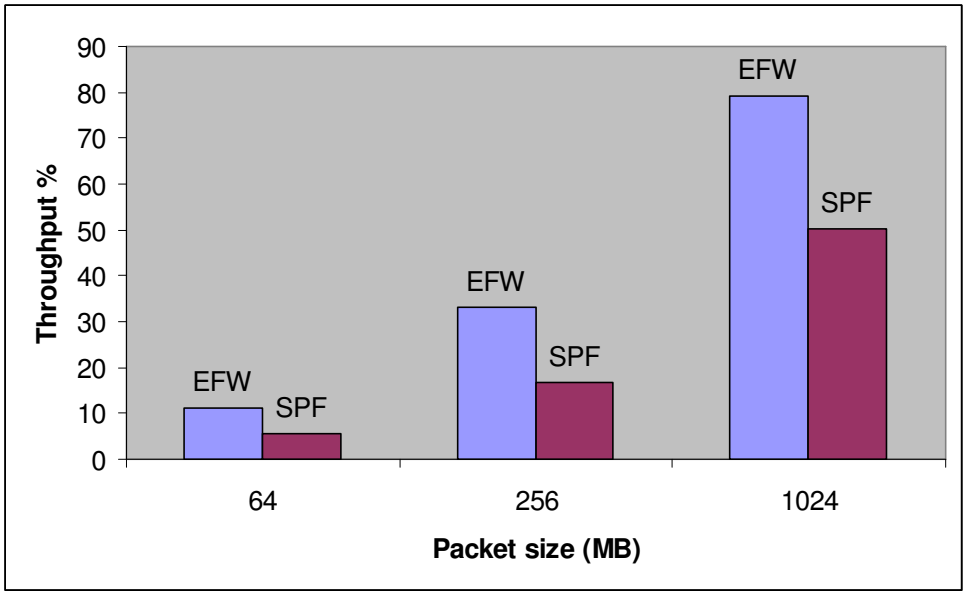

Figure 13. Maximum throughput percentage achieved before any packet loss with UDP

5. Roaming Test

Packet loss test is repeated with the laptop using an EFW PC card, or "roaming device" by 3COM definition. EFW system has two types of PC cards with firewall capability that may be plugged into a laptop: 3COM 3CRFW102 and 3RFW103. 3CRFW102 is using an interface cable for Ethernet whereas 3CRFW103 can accept an Ethernet connection via the port embedded to NIC.

Two laptops are used as EFW clients in roaming test experiment: A Dell Inspiron 5100 with Pentium IV at 2.8 GHz and 384 MB RAM. An IBM Think Pad with Pentium IV at 2.2 GHz and 256 MB RAM. Windows XP Professional Service Pack 1 is installed on each laptop. IBM laptop has an integrated Intel PRC 100/VE NIC, the same model used in comparison of desktop NIC.

TTCP test is performed on the roaming NIC in order to find baseline throughput. No ACL rule is defined in application firewall and EFW NIC is not associated with Policy Server. Figure 14 shows the baseline TCP throughput results of roaming NIC and integrated Intel PRO/100 VE card.

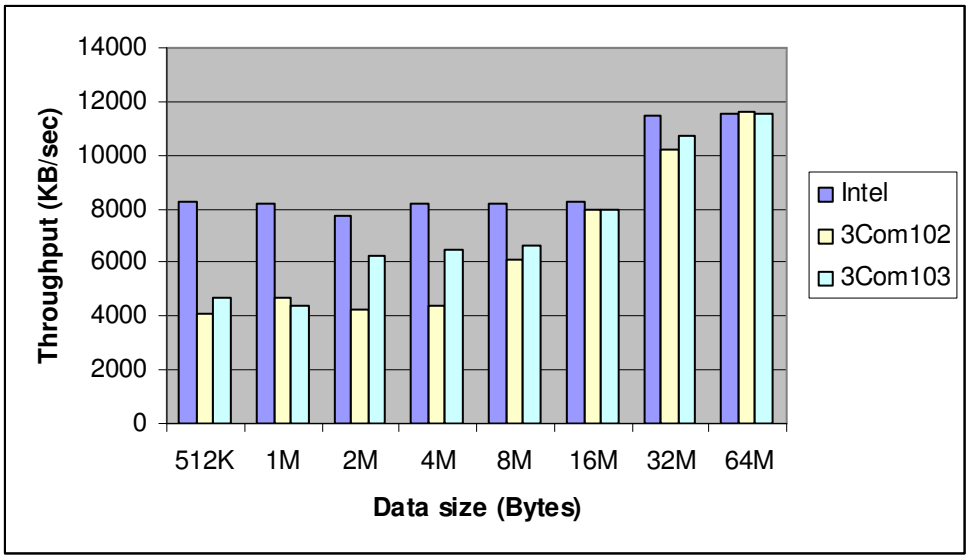

Figure 14. Baseline throughput (KB/sec) of roaming NIC

Results in the Figure 14 imply that 3CRFW102 and 3RFW103 NIC reach their maximum throughput at larger buffer lengths. The results are similar to the results of stationary NIC shown earlier in Figure 7.

Also, TCP throughput tests performed on roaming devices. Similar to throughput tests with stationary NICs, Intel NIC is used with SPF in order to have a more realistic comparison platform. The results show that throughput of roaming devices are not as high as the integrated Intel NIC. The standard deviation of the results is 1207 KB/second whereas the standard deviation for the stationary devices is 0.96 KB/second. PC card interface used in roaming devices is probably primary reason of throughput loss and increase in the variance. Figure 15 below shows the results of roaming device throughput test results.

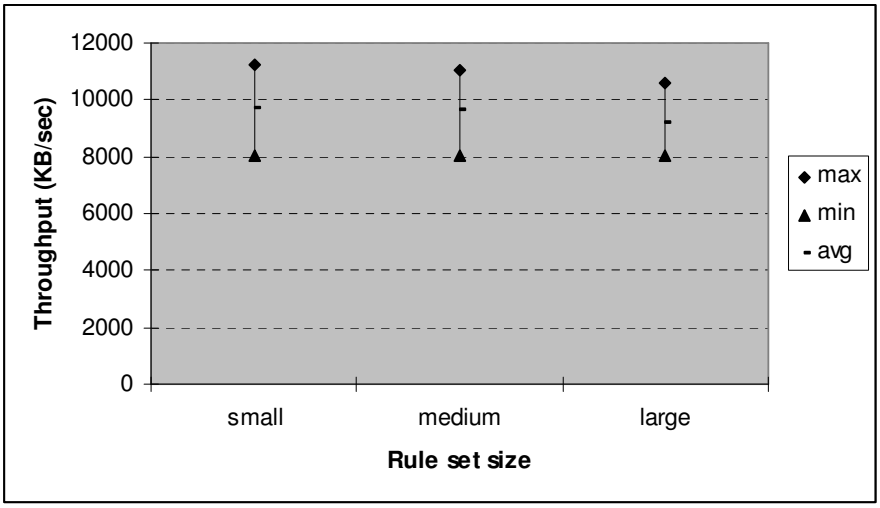

Figure 15. Throughput (KB/second) of roaming devices

The same frame loss test applied to stationary EFW NIC via Smartbits packet generator is applied to EFW with 3RFW102 NIC as well. Integrated Intel NIC is used for SPF system. Large size policy is applied to both EFW and SPF. The packet size changed between 64 and 1024 bytes. The test is performed with both ICMP and UDP packets. NDP of EFW NIC and Intel NIC are calculated by using TCL script. Figure 16 and 17 below shows the frame loss test results of roaming devices.

The NDP values from frame loss test with roaming devices is similar to stationary EFW devices when ICMP is used, whereas NDP values obtained by using UDP are significantly less than stationary EFW devices. However, EFW has larger NDP values than SPF with both ICMP and UDP.

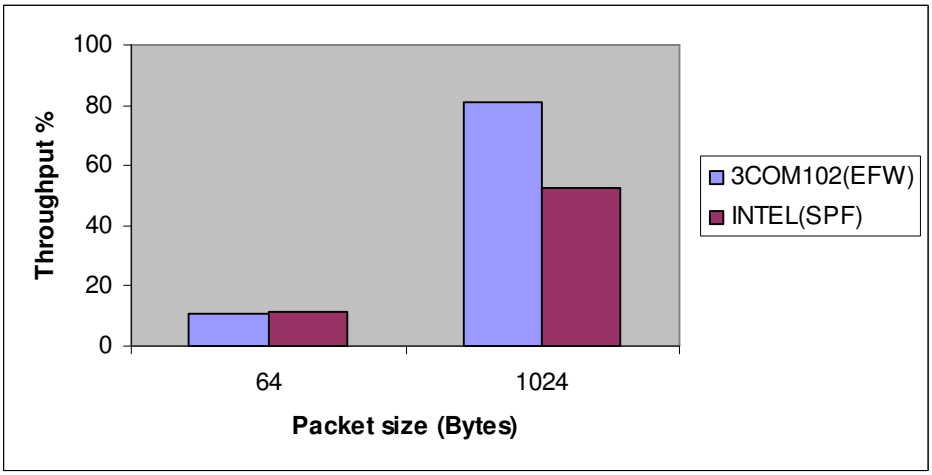

Figure 16. NDP of EFW and SPF of roaming NIC with ICMP

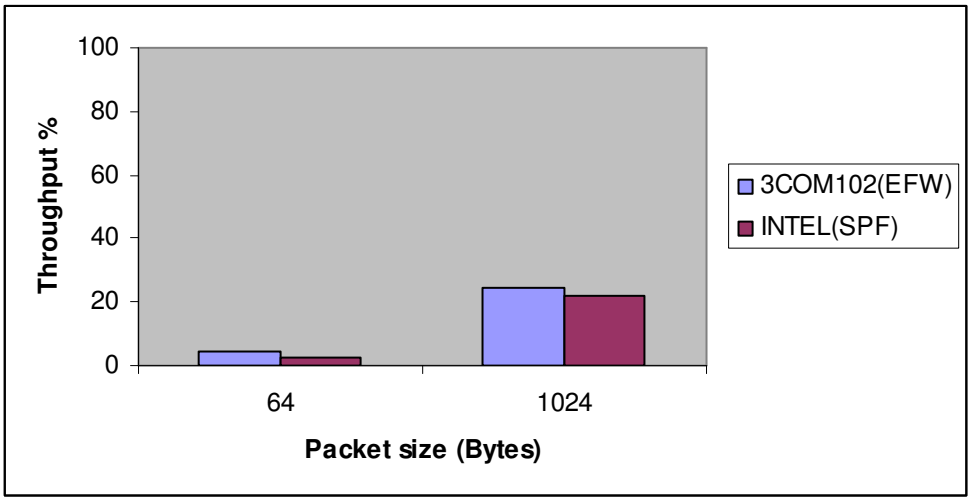

Figure 17. NDP of EFW and SPF of roaming NIC with UDP

E. ANALYSIS

EFW is a good beginning for the new generation firewall systems. First of all, embedding the firewall mechanism into the NIC makes it more difficult for an attacker to disable the firewall without physical access to hardware. Performing encryption and decryption process in hardware improves the performance of firewall system especially in highly cryptography involved connections such as IPSEC. Performance of EFW is very good even under heavy load network conditions. Table 2 demonstrates performance test results of EFW as compared to SPF, a representative of the current host-based application layer firewalls. Throughput values are based on TTCP application with 8192 bytes buffer size, and frame loss values are measured via Smartbits packet generator with 1024 bytes frame size.

However, the implementation of 3COM has some limitations. EFW does not have capability to keep track of connections established, so that it does not provide advantages of a stateful firewall. Furthermore, it does not provide some features in today's software oriented firewalls such as SPF, which are capable of performing filtering at higher layers in OSI network model.

Table 2. Performance test results of EFW and SPF systems

Firewall System	Throughput		Frame loss (NDP)	
	TCP	IPSEC	ICMP	UDP
EFW	11554.30 KB/sec	8702.49 KB/sec	93.35 %	79.10 %
SPF	11484.93 KB/sec	5748.81 KB/sec	50.19 %	50.19 %

Even though EFW is integrated well with Windows OS and TCP/IP, there is no support for other OS and networking protocols at the moment. The dependency on Windows limits the scalability of EFW in networks running servers on other types of OS. Enterprise networks using other protocols than TCP/IP cannot depend on EFW as the firewall solution.

Network-based firewalls, serving on layer 2 and 3 in OSI model, can be used effectively with other OS and networking protocols. They still have advantage in performance because processing at lower layers can be done faster than processing at higher layers. Except the ones installed on the routers, network based firewalls generally have a whole hardware system dedicated to only firewall process that increase their performance as well. The network-based firewalls have a disadvantage due to their location in the network security architecture. A large amount of traffic passing through the firewall may cause firewall to become the bottleneck of the network performance. Therefore, adding EFW to the network security system may reduce the amount of traffic passing through the network-based firewall and prevent it from becoming the single point of failure in case of a DOS attack.

EFW system serves on the transport layer and is able to examine the packets in more detail. The key advantage of the EFW system is its ability to prevent insider attacks. The performance of the EFW is very good particularly in high-crypto connections and reasonable at standard connections. The main disadvantage of EFW system is the lack of recollection mechanism for dynamically tracking the connections established. An

application firewall used with EFW system concurrently will maximize the security utilities and performance in firewall architecture.

Application firewalls are the most security capable firewalls because their filtering can be specified at the highest layer in the OSI model. Some of the application firewalls also have IDS capabilities so they can address more sophisticated attacks. Since, application firewalls are based on software rather than hardware, their performance is weaker than other firewall systems. Carefully defining the ACL of an application firewall is the best solution for getting highest benefit from its security utilities.

Table 3 below compares the security capabilities of network-based and host-based firewalls including EFW.

Table 3. Security capabilities of firewall systems

Firewall System	**Filtering layer**	**Recollection**	**Location**
Network-based FW	Network (layer 3)	No	Network gateway
EFW	Transport (layer 4)	No	Host NIC
Application FW	Application (layer7)	Yes	Host

Defense-in-depth approach is gaining more support as security concept of modern networking. The idea behind this concept is relying on the intelligent application of techniques that exist today. The strategy followed suggests having a balance between the protection and cost.

The EFW system can play an important role in a defense-in-depth implementation. Application firewalls such as SPF and IDS applications can be used together with EFW. Such a configuration merges the performance advantage of EFW in crypto-heavy connections especially and security capabilities of software-based security systems. Both insider and outsider threats will be addressed in this implementation. The application firewall will not add a large amount of cost to the EFW system. In this research performance of such a configuration consisted of SPF and EFW is tested.

Results of the test indicate that SPF does not affect the performance gained with EFW NIC in average. Figure 18 below shows the packet loss test results. There are three bars showing the NDPs of SPF, EFW and EFW-SPF configurations from left to right respectively. In the EFW-SPF configuration EFW NIC is used and the large policy rules are applied to both SPF and EFW systems.

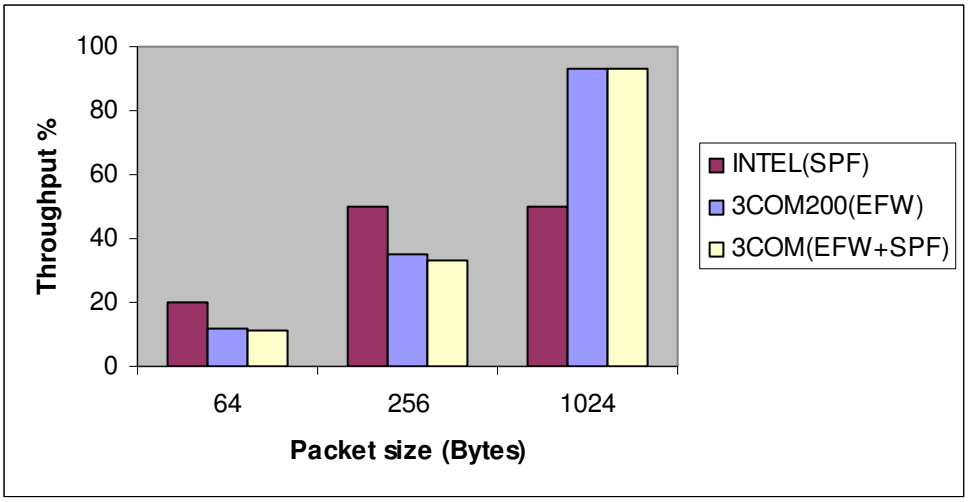

Figure 18. Packet loss percentage of EFW and SPF systems

Besides an application firewall, a network-based firewall may also be used in implementing a defense-in-depth strategy. Network based firewalls will work faster because they do not examine data above layer 3 of the OSI model. Since most of the network protocols accommodated by using layer 3 and below, network-based firewalls can be used nearly at any type of networks. [Wack2002] An EFW protected network may share network-based firewall with an Asynchronous Transfer Mode (ATM) network for example.

In such a configuration consisting of three firewall systems (application firewall, EFW and network-based firewall) filtering task will be divided among the firewalls. A network-based firewall sitting on the gateway router can block certain type of attacks, possibly filter unwanted protocols, perform simple access control and then pass the traffic onto EFW and application firewalls which will examine higher layers of the OSI stack. The performance of the network-based firewall will be high unless it becomes the bottleneck due to large amount of traffic as we discussed previously. The performance on

the hosts will be less compared to gateway, but smaller size of the traffic per host will compensate the performance loss. Figure 19 shows the firewall coverage on the OSI stack.

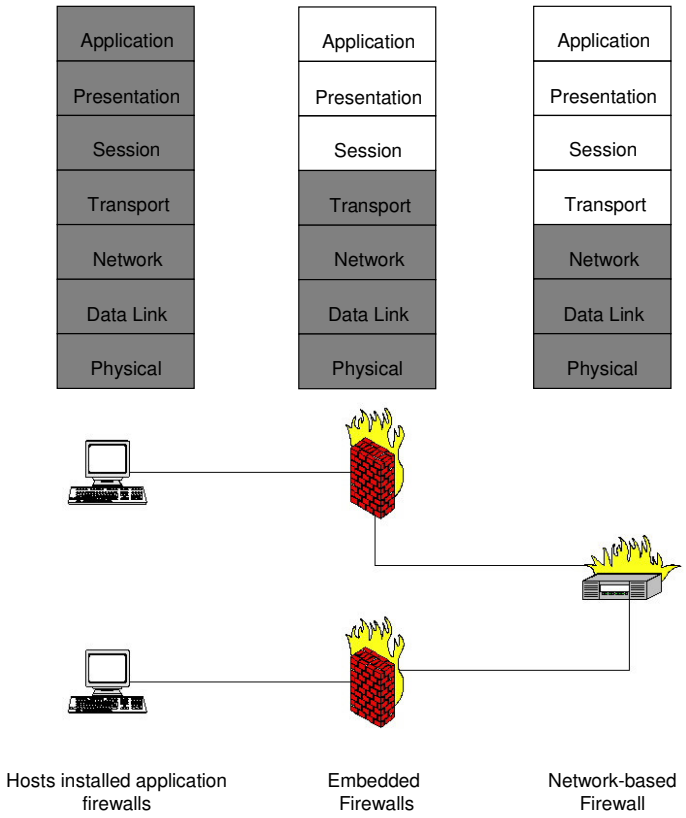

Figure 19. OSI stack coverage of firewall systems

Additionally, some extra adjustment needed in order to let EFW keep its self-control mechanism operational in an integrated configuration with other firewall systems. Two ports (2081, 2082) are used mainly between Policy Server and EFW client applications in order to change policy and configuration information. Application firewalls should let these ports to be used by EFW. If Policy Server and Management Console are at different sides of a network-based firewall, they need to use three more TCP ports in order to maintain connection (2072, 2073, and 2074). At that point, using proxies seems like a good security point.

Configuration of EFW in such an integrated firewall environment depends on multiple factors: size of the network to be protected, amount of traffic, sensitivity of the data etc. A small-scale network without much number of servers may have one Policy Server and EFW clients as many as needed, staying in the recommended limit of 1000 per Policy Server. Based on the expected traffic load, a small-scale network may have a gateway router with a built-in firewall, which will decrease cost of having standalone firewall hardware. EFW clients may have an additional application firewall such as SPF in order to increase layer of filtering, and an IDS as well. Figure 20 below presents an example EFW configuration for a small-scale network.

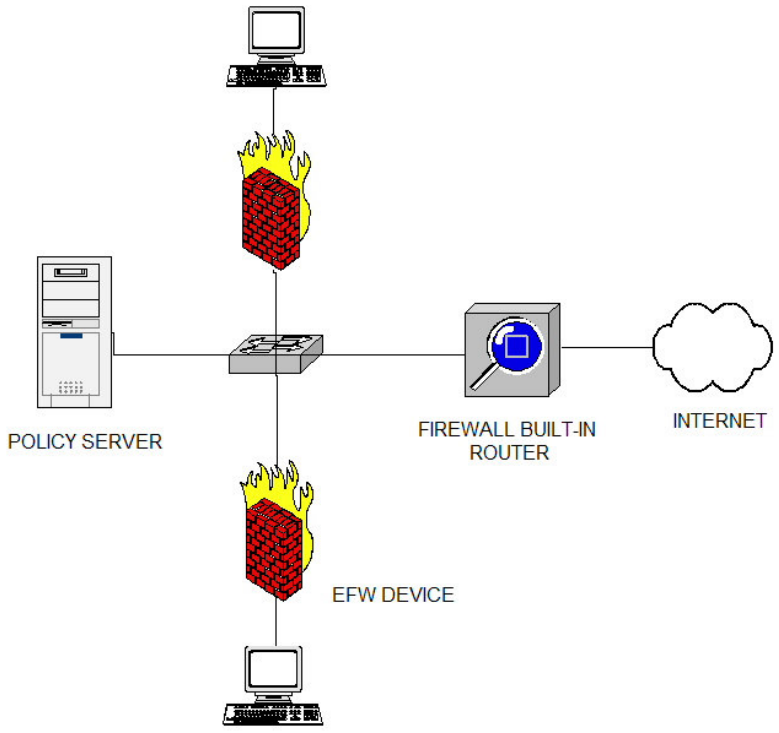

Figure 20. An example of a small-scale EFW configuration

A large-scale network configuration would probably need multiple EFW domains. Having multiple domains controlled by different Policy Servers will provide advantage of assigning different policies according to data sensitivity and threat probability in the particular domain. If the amount of the traffic is as large as the size of the network or if there are multiple sub-networks using other protocols than TCP/IP, a dedicated layer 2 or

3 hardware firewall may be installed at the gateway of the network for increasing performance. Application firewalls and IDSs should be in the configuration to address other security gaps as well. However, one should not ignore that the more the configuration gets complex the more the possibility of configuration-fault increases. Firewall management is as important as implementation of the firewall system, as it is for the other security systems. Figure 21 shows an example EFW deployment in a large-scale network. Domain B, having a database server, will need a more restricted policy than domain A in the example configuration. Web Server is left out of any domain in order to prevent decrease in the performance as if it is in a DMZ.

Besides the management of complex firewall deployments, evaluating these configurations is very time and effort consuming. Parameters and factors for evaluation EFW in this research are selected based on assumption that EFW is a host-based firewall so that traffic passing through it is for only one PC. However, evaluating a network-based firewall will need to examine more factors, and an integrated firewall configuration will need even much more. “Concurrent TCP connection capacity” is one factor suggested in RFC 3511, that we don’t think important for a host-based firewall. For a network based firewall protecting several web servers however, even “TCP tear down time” is an important factor if you imagine the number of HTTP requests dropped during the tear down time at a rush hour. The list of recommended factors in RFC 3511 may be found at Chapter 4 Section F.

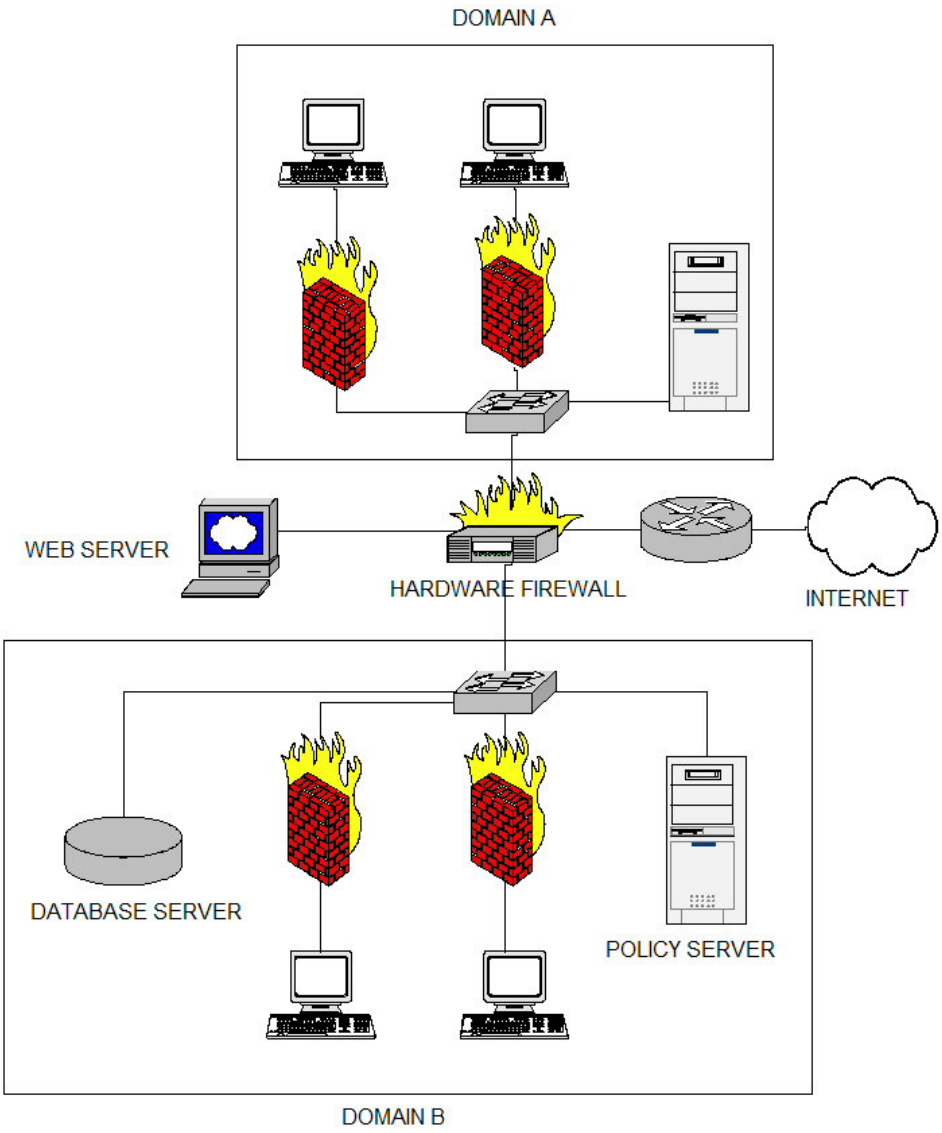

Figure 21. An example of a large-scale EFW configuration

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SUMMARY

A. SUMMARY

In this research EFW system is evaluated by testing it in a network environment set up at the Naval Postgraduate School Advanced Network Laboratory. EFW is a newly developed host-based firewall system that has a solution for one of the most important limitations of firewalls, preventing insider attacks. The research followed the methodology and standardization offered for firewall performance analysis by RFC 2647 and RFC 3511, when applicable.

Firewalls are naturally changing due to the needs emerging from newly discovered vulnerabilities and threats. One of these threats that challenge the old fashioned firewalls is the possibility of attack from the inside. Lately developed firewall systems have software components located at hosts of the network in order to solve insider attack problem. However managing a complex software firewall system is a difficult task. Moreover, putting all these functionalities into one security system generates trade-off between functionality and performance.

EFW is proposed as a combination of host-based and hardware firewalls that merge advantages of two firewall systems. The architecture of EFW is consisted of four main components. These are the Policy Server, the Management Console, EFW devices and the domain that contains one or more of other components. Policy Servers communicate with clients who have EFW devices to exchange information related to firewall operations.

Previous study of EFW done at NPS [Burrows2004] has shown some vulnerability and performance characteristics of the current EFW system. In this research, we extended previous work in both performance and security testing. EFW system is compared with SPF as a representative of application firewall systems. The security testing aims to find vulnerabilities during attempts to penetrate the system whereas the performance testing defines the parameters, factors and metrics that are important to the system.

Scanning performed via NMAP in security tests show that EFW is able to prevent TCP SYN flood and port scans, which needs transport layer filtering capability. However, additional result show that EFW does leave some ports open for NMAP scan, confirming that EFW does not keeps track of states of the connections, thus not a stateful firewall. On the other hand, SPF is able to discard any packet that is not related with a previously established connection.

An important feature of firewalls is the layer that they are able to do filtering. During security testing we tested that EFW does the filtering at transport layer, EFW cannot perform filtering beyond IP header, e.g. at the application layer. SPF looks inside the payload of the packets and decides whether it should let packet to pass through based on the related application's privileges.

Throughput tests in performance testing indicate that performance of EFW and SPF is very close during normal traffic, except that SPF throughput results have more variation. However, EFW has a significant throughput advantage in IPSEC connection. Off-loading mechanism helps to get approximately 25% more throughput by taking the encryption and decryption work from the host CPU.

Throughput results also indicate that the number of the rules in ACL does not affect performance of the firewalls with today's powerful computing resources. Most of the firewall ACL has no more than a hundred rules. Access of firewall to data inside of an IP packet takes a sensible time. However, after reading header information, a linear process of comparing particular fields with less than a hundreds of ACL rules does not take much time. Therefore, access time has more effect than process time on performance of a firewall.

Frame loss tests performed via Smartbits packet generator illustrate performance of EFW significantly better than application firewalls when traffic gets heavy in the network. Contrary to ACL size, the average frame size affects firewall performance considerably. Larger packet size in average leads to better performance. Frame loss test results also indicate that EFW is probably limiting the responses to ICMP echo request bursts. As a result, using UDP in frame loss tests provides more accurate results.

EFW system has special NIC for different platforms. PC card NIC, defined as roaming device in EFW system, is used for laptops that can be integrated into an EFW protected network. TTCP throughput and Smartbits frame loss tests show that roaming devices has similar performance to the stationary EFW devices.

B. FUTURE WORK

Our analysis demonstrates that performance and security trade-off between firewall systems still holds its important effect in design principles. We propose to integrate EFW system with network-based firewalls and application firewalls, in a defense-in-depth scheme. One should note that EFW system's key advantage on such integration is ability to address insider attacks. However, EFW system has a couple of weaknesses that needs to be reviewed before taking place in the configurations which we proposed. Configuration of EFW in such an integrated deployment will be based on different factors. Some important factors are size of the network, amount of traffic and sensitivity of data.

Based on the analysis we did, there are still needs for further study on how to create a best network configuration that maximizes the utility, performance and resistance to insider attacks. A firewall configuration including a network-based firewall will have to protect some servers besides client computers. Latency distribution over time and support of different connection types are among the important parameters for servers. A network-based firewall should not be a bottleneck for server traffic through the networks. Therefore, more factors such as the number of possible concurrent connections and connection establishment / tear down rate should be considered when evaluating such an integrated firewall system.

Traffic generated on higher layers of the OSI model will not be appropriate for measuring the network-based firewall performance. Performance analysis software applications are appropriate for measuring firewalls working at higher layers. We used TTCP as the network performance analysis application in this research. TTCP use transport layer protocols TCP and UDP to measure the throughput of DUT/SUT. Smartbits hardware based packet generator used for packet loss tests will be more

effective in measuring the performance at lower layers in the OSI model. Additionally, using a hardware packet generator will provide a wider platform to compare different firewall system architectures.

APPENDIX A. STATISTICS DATA

Table 4. TCP throughput (KB/sec) results of NIC via TTCP

	Stationary			Roaming		
Buffer length	Intel	3Com200	3Com920	Intel	3Com102	3Com103
256	10893.62	8258.6	8258.6	8258.06	4096	4697.25
512	10893.62	9394.5	8192	8192	4697.25	4357.45
1024	10951.87	8192	8192	7728.3	4231.4	6243.9
2048	11409.47	7937.98	7937.98	8192	4371.4	6496.43
4096	11393.6	8062.99	7824.26	8192	6099.78	6633.2
8192	11521.8	8003.91	8003.91	8253.9	7945.68	8003.91
16384	11461.35	11461.35	11521.8	11461.35	10224.02	10701.5
32768	11521.8	11521.8	11586.99	11554.3	11584.94	11554.3

Table 5. TCP throughput (KB/second) with different size of rule sets applied.

	EFW			SPF		
RUN	Small	Medium	Large	Small	Medium	Large
Run1	11554.3	11554.3	11554.3	11529.91	11521.8	11521.8
Run2	11554.3	11554.3	11554.3	11652.92	11521.8	11401.53
Run3	11554.3	11554.3	11554.3	11652.92	11521.8	11521.8
Run4	11554.3	11554.3	11554.3	11521.8	11529.91	11401.53
Run5	11554.3	11554.3	11554.3	11521.8	11393.6	11521.8
Run6	11554.3	11554.3	11554.3	11521.8	11521.8	11393.6
Run7	11554.3	11554.3	11554.3	11521.8	11521.8	11521.8
Run8	11556.34	11554.3	11554.3	11521.8	11521.8	11521.8
Run9	11556.34	11554.3	11554.3	11521.8	11521.8	11521.8
Run10	11556.34	11554.3	11554.3	11521.8	11521.8	11521.8
Average	11554.91	11554.3	11554.3	11548.84	11509.79	11484.93
Maximum	11556.34	11554.3	11554.3	11652.92	11529.91	11521.8

Table 6. Throughput (KB/seconds) of firewalls with IPSEC

RUN	SPF		EFW	
	w/ IPSEC	w/o IPSEC	w/ IPSEC	w/o IPSEC
Run1	11521.8	5992.68	11554.3	8289.4
Run2	11401.53	5957.82	11554.3	8702.16
Run3	11521.8	4923.08	11554.3	8701.01
Run4	11401.53	5992.68	11554.3	8756.81
Run5	11521.8	5957.82	11554.3	8738.13
Run6	11393.6	4899.52	11554.3	8720.69
Run7	11521.8	5925.5	11554.3	8793.24
Run8	11521.8	5923.36	11554.3	8774.4
Run9	11521.8	5957.82	11554.3	8738.13
Run10	11521.8	5957.82	11554.3	8810.97
Average	11484.93	5748.81	11554.3	8702.494

Table 7. Packet loss test results of stationary EFW using ICMP packets

Packet Length	Packets/ Second	Bytes/ Second	Percent Bandwidth	Packets Sent	Packets Received	Bytes Sent	Bytes Received	Pct Received
64	14204	965872	10	42612	42721	2897616	2905028	100.26
64	28409	1931812	20	85227	50833	5795436	3456644	59.64
64	42662	2901016	30	127986	51927	8703048	3531036	40.57
64	56818	3863624	40	170454	52833	11590872	3592644	31
64	71022	4829496	50	213066	53951	14488488	3668668	25.32
64	85616	5821888	60	256848	3860	17465664	262480	1.5
64	100000	6800000	70	300000	634	20400000	43112	0.21
64	113636	7727248	80	340908	630	23181744	42840	0.18
64	128865	8762820	90	386595	581	26288460	39508	0.15
64	142045	9659060	100	426135	674	28977180	45832	0.16
256	4464	1160640	10	13392	13542	3481920	3520920	101.12
256	8928	2321280	20	26784	26784	6963840	6963840	100
256	13397	3483220	30	40191	41635	10449660	10825100	103.59
256	17857	4642820	40	53571	45860	13928460	11923600	85.61
256	22321	5803460	50	66963	45053	17410380	11713780	67.28
256	26824	6974240	60	80472	44801	20922720	11648260	55.67
256	31250	8125000	70	93750	44837	24375000	11657620	47.83
256	35714	9285640	80	107142	3000	27856920	780000	2.8
256	40192	10449920	90	120576	171	31349760	44460	0.14
256	44642	11606920	100	133926	276	34820760	71760	0.21

1024	1192	1225376	10	3576	3581	3676128	3681268	100.14
1024	2385	2451780	20	7155	7177	7355340	7377956	100.31
1024	3578	3678184	30	10734	10763	11034552	11064364	100.27
1024	4770	4903560	40	14310	14368	14710680	14770304	100.41
1024	5963	6129964	50	17889	17889	18389892	18389892	100
1024	7159	7359452	60	21477	21477	22078356	22078356	100
1024	8350	8583800	70	25050	25050	25751400	25751400	100
1024	9541	9808148	80	28623	28623	29424444	29424444	100
1024	10738	11038664	90	32214	32215	33115992	33117020	100
1024	11927	12260956	100	35781	110	36782868	113080	0.31

Table 8. Packet loss test results of stationary SPF using ICMP packets

Packet Length	Packets/ Second	Bytes/ Second	Percent Bandwidth	Packets Sent	Packets Received	Bytes Sent	Bytes Received	Pct Received
64	14204	965872	10	42612	42612	2897616	2897616	100
64	28409	1931812	20	85227	49065	5795436	3336420	57.57
64	42662	2901016	30	127986	50127	8703048	3408636	39.17
64	56818	3863624	40	170454	51081	11590872	3473508	29.97
64	71022	4829496	50	213066	52152	14488488	3546336	24.48
64	85616	5821888	60	256848	3846	17465664	261528	1.5
64	100000	6800000	70	300000	641	20400000	43588	0.21
64	113636	7727248	80	340908	609	23181744	41412	0.18
64	128865	8762820	90	386595	593	26288460	40324	0.15
64	142045	9659060	100	426135	668	28977180	45424	0.16
256	4464	1160640	10	13392	13549	3481920	3522740	101.17
256	8928	2321280	20	26784	26784	6963840	6963840	100
256	13397	3483220	30	40191	41372	10449660	10756720	102.94
256	17857	4642820	40	53571	44447	13928460	11556220	82.97
256	22321	5803460	50	66963	43760	17410380	11377600	65.35
256	26824	6974240	60	80472	43323	20922720	11263980	53.84
256	31250	8125000	70	93750	43364	24375000	11274640	46.25
256	35714	9285640	80	107142	3073	27856920	798980	2.87
256	40192	10449920	90	120576	233	31349760	60580	0.19
256	44642	11606920	100	133926	274	34820760	71240	0.2
1024	1192	1225376	10	3576	3581	3676128	3681268	100.14

1024	2385	2451780	20	7155	7195	7355340	7396460	100.56
1024	3578	3678184	30	10734	10802	11034552	11104456	100.63
1024	4770	4903560	40	14310	14359	14710680	14761052	100.34
1024	5963	6129964	50	17889	17889	18389892	18389892	100
1024	7159	7359452	60	21477	21477	22078356	22078356	100
1024	8350	8583800	70	25050	25050	25751400	25751400	100
1024	9541	9808148	80	28623	28369	29424444	29163332	99.11
1024	10738	11038664	90	32214	28529	33115992	29327812	88.56
1024	11927	12260956	100	35781	100	36782868	102800	0.28

Table 9. Packet loss test results of stationary EFW using UDP packets

Packet Length	Packets/ Second	Bytes/ Second	Percent Bandwidth	Packets Sent	Packets Received	Bytes Sent	Bytes Received	Pct Received
64	14204	965872	10	42612	42613	2897616	2897684	100
64	28409	1931812	20	85227	82323	5795436	5597964	96.59
64	42662	2901016	30	127986	86702	8703048	5895736	67.74
64	56818	3863624	40	170454	88895	11590872	6044860	52.15
64	71022	4829496	50	213066	90307	14488488	6140876	42.38
64	85616	5821888	60	256848	257833	17465664	17532644	100.38
64	100000	6800000	70	300000	1304	20400000	88672	0.43
64	113636	7727248	80	340908	1304	23181744	88672	0.38
64	128865	8762820	90	386595	1305	26288460	88740	0.34
64	142045	9659060	100	426135	1305	28977180	88740	0.31
256	4464	1160640	10	13392	13392	3481920	3481920	100
256	8928	2321280	20	26784	26784	6963840	6963840	100
256	13397	3483220	30	40191	40377	10449660	10498020	100.46
256	17857	4642820	40	53571	53590	13928460	13933400	100.04
256	22321	5803460	50	66963	66653	17410380	17329780	99.54
256	26824	6974240	60	80472	68816	20922720	17892160	85.52
256	31250	8125000	70	93750	70170	24375000	18244200	74.85
256	35714	9285640	80	107142	13340	27856920	3468400	12.45
256	40192	10449920	90	120576	1120	31349760	291200	0.93
256	44642	11606920	100	133926	1130	34820760	293800	0.84

1024	1192	1225376	10	3576	3576	3676128	3676128	100
1024	2385	2451780	20	7155	7160	7355340	7360480	100.07
1024	3578	3678184	30	10734	10734	11034552	11034552	100
1024	4770	4903560	40	14310	14310	14710680	14710680	100
1024	5963	6129964	50	17889	17889	18389892	18389892	100
1024	7159	7359452	60	21477	3411	22078356	3506508	15.88
1024	8350	8583800	70	25050	3488	25751400	3585664	13.92
1024	9541	9808148	80	28623	3431	29424444	3527068	11.99
1024	10738	11038664	90	32214	3513	33115992	3611364	10.91
1024	11927	12260956	100	35781	1053	36782868	1082484	2.94

Table 10. Packet loss test results of stationary SPF using UDP packets

Packet Length	Packets/ Second	Bytes/ Second	Percent Bandwidth	Packets Sent	Packets Received	Bytes Sent	Bytes Received	Pct Received
64	14204	965872	10	42612	15224	2897616	1035232	35.73
64	28409	1931812	20	85227	12554	5795436	853672	14.73
64	42662	2901016	30	127986	15195	8703048	1033260	11.87
64	56818	3863624	40	170454	13791	11590872	937788	8.09
64	71022	4829496	50	213066	13998	14488488	951864	6.57
64	85616	5821888	60	256848	254967	17465664	17337756	99.27
64	100000	6800000	70	300000	1838	20400000	124984	0.61
64	113636	7727248	80	340908	1680	23181744	114240	0.49
64	128865	8762820	90	386595	922	26288460	62696	0.24
64	142045	9659060	100	426135	1165	28977180	79220	0.27
256	4464	1160640	10	13392	13392	3481920	3481920	100
256	8928	2321280	20	26784	20424	6963840	5310240	76.25
256	13397	3483220	30	40191	11948	10449660	3106480	29.73
256	17857	4642820	40	53571	7683	13928460	1997580	14.34
256	22321	5803460	50	66963	6154	17410380	1600040	9.19
256	26824	6974240	60	80472	6949	20922720	1806740	8.64
256	31250	8125000	70	93750	6359	24375000	1653340	6.78
256	35714	9285640	80	107142	105713	27856920	27485380	98.67
256	40192	10449920	90	120576	159	31349760	41340	0.13
256	44642	11606920	100	133926	243	34820760	63180	0.18
1024	1192	1225376	10	3576	3576	3676128	3676128	100

1024	2385	2451780	20	7155	7155	7355340	7355340	100
1024	3578	3678184	30	10734	10734	11034552	11034552	100
1024	4770	4903560	40	14310	14310	14710680	14710680	100
1024	5963	6129964	50	17889	17889	18389892	18389892	100
1024	7159	7359452	60	21477	2500	22078356	2570000	11.64
1024	8350	8583800	70	25050	2518	25751400	2588504	10.05
1024	9541	9808148	80	28623	2467	29424444	2536076	8.62
1024	10738	11038664	90	32214	2447	33115992	2515516	7.6
1024	11927	12260956	100	35781	68	36782868	69904	0.19

Table 11. Packet loss test results of roaming EFW device with ICMP packets

Packet Length	Packets/ Second	Bytes/ Second	Percent Bandwidth	Packets Sent	Packets Received	Bytes Sent	Bytes Received	Pct Received
64	14204	965872	10	42612	42883	2897616	2916044	100.64
64	28409	1931812	20	85227	45014	5795436	3060952	52.82
64	42662	2901016	30	127986	47701	8703048	3243668	37.27
64	56818	3863624	40	170454	48687	11590872	3310716	28.56
64	71022	4829496	50	213066	49656	14488488	3376608	23.31
64	85616	5821888	60	256848	3942	17465664	268056	1.53
64	100000	6800000	70	300000	634	20400000	43112	0.21
64	113636	7727248	80	340908	617	23181744	41956	0.18
64	128865	8762820	90	386595	613	26288460	41684	0.16
64	142045	9659060	100	426135	665	28977180	45220	0.16
256	4464	1160640	10	13392	13530	3481920	3517800	101.03
256	8928	2321280	20	26784	26784	6963840	6963840	100
256	13397	3483220	30	40191	41694	10449660	10840440	103.74
256	17857	4642820	40	53571	42075	13928460	10939500	78.54
256	22321	5803460	50	66963	41703	17410380	10842780	62.28
256	26824	6974240	60	80472	41017	20922720	10664420	50.97
256	31250	8125000	70	93750	41083	24375000	10681580	43.82
256	35714	9285640	80	107142	3101	27856920	806260	2.89
256	40192	10449920	90	120576	197	31349760	51220	0.16
256	44642	11606920	100	133926	270	34820760	70200	0.2

1024	1192	1225376	10	3576	3583	3676128	3683324	100.2
1024	2385	2451780	20	7155	7157	7355340	7357396	100.03
1024	3578	3678184	30	10734	10765	11034552	11066420	100.29
1024	4770	4903560	40	14310	14313	14710680	14713764	100.02
1024	5963	6129964	50	17889	17889	18389892	18389892	100
1024	7159	7359452	60	21477	21477	22078356	22078356	100
1024	8350	8583800	70	25050	25050	25751400	25751400	100
1024	9541	9808148	80	28623	28624	29424444	29425472	100
1024	10738	11038664	90	32214	32200	33115992	33101600	99.96
1024	11927	12260956	100	35781	180	36782868	185040	0.5

Table 12. Packet loss test results of roaming EFW device with UDP packets

Packet Length	Packets/ Second	Bytes/ Second	Percent Bandwidth	Packets Sent	Packets Received	Bytes Sent	Bytes Received	Pct Received
64	14204	965872	10	42612	2822	2897616	191896	6.62
64	28409	1931812	20	85227	374	5795436	25432	0.44
64	42662	2901016	30	127986	374	8703048	25432	0.29
64	56818	3863624	40	170454	374	11590872	25432	0.22
64	71022	4829496	50	213066	374	14488488	25432	0.18
64	85616	5821888	60	256848	374	17465664	25432	0.15
64	100000	6800000	70	300000	374	20400000	25432	0.12
64	113636	7727248	80	340908	374	23181744	25432	0.11
64	128865	8762820	90	386595	374	26288460	25432	0.1
64	142045	9659060	100	426135	374	28977180	25432	0.09
256	4464	1160640	10	13392	13470	3481920	3502200	100.58
256	8928	2321280	20	26784	7748	6963840	2014480	28.93
256	13397	3483220	30	40191	2787	10449660	724620	6.93
256	17857	4642820	40	53571	40	13928460	10400	0.07
256	22321	5803460	50	66963	40	17410380	10400	0.06
256	26824	6974240	60	80472	40	20922720	10400	0.05
256	31250	8125000	70	93750	40	24375000	10400	0.04
256	35714	9285640	80	107142	40	27856920	10400	0.04
256	40192	10449920	90	120576	40	31349760	10400	0.03
256	44642	11606920	100	133926	40	34820760	10400	0.03
1024	1192	1225376	10	3576	3582	3676128	3682296	100.17

1024	2385	2451780	20	7155	7161	7355340	7361508	100.08
1024	3578	3678184	30	10734	10728	11034552	11028384	99.94
1024	4770	4903560	40	14310	12214	14710680	12555992	85.35
1024	5963	6129964	50	17889	7545	18389892	7756260	42.18
1024	7159	7359452	60	21477	10091	22078356	10373548	46.99
1024	8350	8583800	70	25050	7969	25751400	8192132	31.81
1024	9541	9808148	80	28623	10	29424444	10280	0.03
1024	10738	11038664	90	32214	10	33115992	10280	0.03
1024	11927	12260956	100	35781	59	36782868	60652	0.16

Table 13. No drop point test results of EFW

Packet Length	Packets/ Second	Bytes/ Second	Percent Bandwidth	Packets Sent	Packets Received	Bytes Sent	Bytes Received
ICMP	64	1133288	11.71875	49998	3399864	3399864	100
ICMP	256	4037020	34.76563	46581	12111060	12703080	104.89
ICMP	1024	11451920	93.35938	33420	34355760	34391740	100.1
UDP	64	1075896	11.13281	47466	3227688	3227756	100
UDP	256	3832400	33.00781	44220	11497200	11961820	104.04
UDP	1024	9705348	79.10156	28323	29116044	29116044	100

Table 14. No drop point test results of SPF

Packet Length	Packets/ Second	Bytes/ Second	Percent Bandwidth	Packets Sent	Packets Received	Bytes Sent	Bytes Received
ICMP	64	1945072	20.11719	85812	5835216	5868128	100.56
ICMP	256	5803460	50	66963	17410380	17410640	100
ICMP	1024	6156692	50.19531	17967	18470076	18470076	100
UDP	64	547264	5.664063	24144	1641792	1663892	101.35
UDP	256	1950780	16.79688	22509	5852340	5868200	100.27
UDP	1024	6156692	50.19531	17967	18470076	18470076	100

APPENDIX B. FIREWALL RULE SETS

Table 15. Small firewall rule set.

Action	Source	Port	Destination	Port	Protocol	Comment
Allow	Any	Any	Any	Any	Any	Allow ALL

Table 16. Medium firewall rule set.

Action	Source	Port	Destination	Port	Protocol	Comment
Allow	Any	Any	[Host]	Any	ICMP	Inbound ICMP
Allow	[Host]	Any	Any	Any	ICMP	Outbound ICMP
Allow	Any	Any	[Host]	Any	TCP	Inbound TCP
Allow	[Host]	Any	Any	Any	TCP	Outbound TCP
Block	Any	Any	Any	Any	Any	Block ALL

Table 17. Large firewall rule set.

Action	Source	Port	Destination	Port	Protocol	Comment
Allow	Any	Any	[Host]	Any	ICMP	Inbound ICMP
Allow	[Host]	Any	Any	Any	ICMP	Outbound ICMP
Allow	Any	53	[Host]	Any	UDP	Inbound DNS
Allow	[Host]	Any	Any	53	TCP	Outbound DNS
Allow	[Host]	Any	Any	53	UDP	Outbound DNS
Allow	[Host]	Any	Any	137	TCP	Outbound NetBIOS
Allow	[Host]	Any	Any	138	TCP	Outbound NetBIOS
Allow	[Host]	Any	Any	139	TCP	Outbound NetBIOS
Allow	[Host]	Any	Any	137	UDP	Outbound NetBIOS
Allow	[Host]	Any	Any	138	UDP	Outbound NetBIOS

Allow	[Host]	Any	Any	139	UDP	Outbound NetBIOS
Block	Any	Any	[Host]	137	TCP	Inbound NetBIOS
Block	Any	Any	[Host]	138	TCP	Inbound NetBIOS
Block	Any	Any	[Host]	139	TCP	Inbound NetBIOS
Block	Any	Any	[Host]	137	UDP	Inbound NetBIOS
Block	Any	Any	[Host]	138	UDP	Inbound NetBIOS
Block	Any	Any	[Host]	139	UDP	Inbound NetBIOS
Allow	Any	Any	127.0.0.1	Any	UDP	Inbound Loop back
Allow	127.0.0.1	Any	Any	Any	TCP	Outbound Loop back
Allow	127.0.0.1	Any	Any	Any	UDP	Outbound Loop back
Block	[Host]	Any	Any	443	TCP	Access to secure sites
Block	Any	Any	[Host]	Any	ICMP	Inbound ICMP
Block	[Host]	Any	Any	Any	ICMP	Outbound ICMP
Allow	Any	Any	[Host]	67	UDP	Inbound Bootp
Allow	Any	Any	[Host]	68	UDP	Inbound Bootp
Allow	[Host]	Any	Any	Any	TCP	Outbound Bootp
Allow	[Host]	Any	Any	Any	UDP	Outbound Bootp
Block	Any	Any	[Host]	445	TCP	Microsoft Windows SMB
Block	Any	Any	[Host]	445	UDP	Microsoft Windows SMB
Block	Any	Any	[Host]	135	TCP	EPMAP
Block	Any	Any	[Host]	135	UDP	EPMAP

LIST OF REFERENCES

[3Com2003] 3Com Corporation. 3Com Embedded Firewall System Administration Guide. Santa Clara, California: 3Com Corporation, 2003

[3Com2004] 3Com Corporation. 3Com Embedded Firewall Solution. Online. March, 2005. Internet. 3Com Products web page. Available: <http://www.3com.com/other/pdfs/products/en_US/400741.pdf> March, 2005.

[Burrows2004] Lemott, and Damon Burrows. "Evaluation of the 3COM® EFW System and its Role in Protection against DDOS Attacks." Master's Thesis. Naval Postgraduate School, 2004.

[Cheswick2003] Rubin, Bellovin, and William R. Cheswick. Firewalls and Internet Security. Florham Park, New Jersey: Addison-Wesley 2003

[Denning2003] Denning, P.J. Great Principles of Computing. Communication of ACM Vol.46 No: 11, November, 2003.

[Geigg2004] Seipp, G. "TTCP—Windows NT/95 Port of TTCP". Online. February, 1997. Internet. North Carolina State University Networking Lab. Available: < http://renoir.csc.ncsu.edu/ttcp/> March, 2005.

[NSA2005] National Security Agency. Defense in Depth. Online. Information Assurance Solution Group. Internet. December, 2004. Available: <http://www.nsa.gov/snac/support/defenseindepth.pdf > March, 2005.

[RFC2401] Kent, S. Security Architecture for Internet Protocol. Online. IETF-RFC. Internet. November, 1998. Available: <http://www.ietf.org/rfc/rfc2401.txt> March, 2005.

[RFC2647] D. Newman. Benchmarking Terminology for Firewall Performance. Online. IETF-RFC. Internet. November, 1998. Available: < http://www.ietf.org/rfc/rfc2647.txt> March, 2005.

[RFC3511] Hickman, Newman, Tadjudin and Martin T. Benchmarking Methodology for Firewall Performance. Online. IETF-RFC. Internet. November, 1998. Available: <http://www.ietf.org/rfc/rfc3511.txt> March, 2005.

[Secure2001] Secure Computing Corporation. Simplified HIPAA compliance using 3COM Embedded Firewall. Online. Secure Computing Corporation web page. Internet. December, 2004. Available:<http://www.securecomputing.com/pdf/EFW_HIPAA_sb.pdf > March, 2005.

[Smith1997] Smith, R. Internet Cryptography. Reading, MA: Addison-Wesley, 1997.

[Spirent2001] Spirent Communications. How to test NIC with echo traffic. Online. Spirent Communications web site. Internet. May, 2001. Available:< http://www.spirentcom.com/documents/162.pdf > March, 2005

[Spirent2003] Spirent Communications. Smartbits 600/6000B/6000C Installation Guide. Washington D.C.: Spirent Communications, August, 2003.

[Stewart2004] Stewart, Dodge and D. Ragsdale. Embedded Firewall Defense. 2nd IEEE Information Assurance workshop. Online. United States Military Academy. Internet. March, 2004. Available: <http://www.itoc.usma.edu/ragsdale/pubs/Embedded_Firewall_Defense_Paper_IA_.pdf> March, 2005.

[Wack2002] Cutler, Pole, and John Wack. Guidelines on Firewalls and Firewall Policy. Online. National Institute of Standards and Technology. Internet. December, 2001. Available: <http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf> March, 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Wen Su
   Naval Postgraduate School
   Computer Science Department
   Monterey, California

4. Dr. Craig Martell
   Naval Postgraduate School
   Computer Science Department
   Monterey, California

5. LT Harold Cole
   Fort George G Meade, Maryland

6. LT Matt Smith
   Fort George G Meade, Maryland