##### STATEFUL INSPECTION FIREWALL USING LINUX

**A PROJECT REPORT**

###### 

###### ***Submitted by***

*in partial fulfillment for the award of the degree*

*of*

##### **BACHELOR OF TECHNOLOGY**

*in*

**COMPUTER SCIENCE AND ENGINEERING**

**CYBER SECURITY and DIGITAL FORENSICS**



**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**VIT BHOPAL UNIVERSITY**

**KOTHRIKALAN, SEHORE**

**MADHYA PRADESH - 466114**

OCTOBER 2020

**VIT BHOPAL UNIVERSITY,KOTHRIKALAN, SEHORE**

**MADHYA PRADESH – 466114**

**LIST OF ABBREVIATIONS**

Sf-Security Features

NAT-Network Address Translation

ip-Internet Protocol

TCP-Transmission Control Protocol

UDP-User Datagram Protocol

NGFW-Next Generation Firewall

IDS-Intrusion Detection System

UTM-Unified Threat Management

**LIST OF FIGURES**

| **No** | **Figure** | **Page Number** |
| --- | --- | --- |
| 1 | Firewall Reference Model | 14 |
| 2 | Figure-1 | 19 |
| 3 | Figure-2 | 20 |
| 4 | Figure-3 | 21 |
| 5 | Figure-4 | 21 |
| 6 | Graph-1 | 23 |
| 7 | Graph-2 | 24 |
| 8 | Graph-3 | 25 |

**LIST OF TABLES**

| **No** | **Table** | **Page Number** |
| --- | --- | --- |
| 1 | Table-1 | 22 |
| 2 | Table-2 | 22 |
| 3 | Table-3 | 23 |

**ABSTRACT**

A firewall is employed as a defence line between a secure network and an unsecure network.In this paper, first we discuss security issues with stateless basic packet filtering, and the concepts of stateful TCP packet filtering.A firewall may act as a packet filter. It can operate as a positive filter, allowing to pass only packets that meet specific criteria, or as a negative filter, rejecting any packet that meets certain criteria.

Depending on the type of firewall, it may examine one or more protocol headers in each packet, the payload of each packet, or the pattern generated by a sequence of packets. A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet. The firewall is typically configured to filter packets going in both directions (from and to the internal network). Filtering rules are based on information contained in a network packet.Filtering policy is set upon a stateless firewall by a network admin,by which all incoming and outgoing packets have to abide by.

The proposed firewall was implemented on CentOS Linux, between a network and a computer connected to the network,following TCP/IP,UDP protocols,with the root user having complete control over the firewall.

**TABLE OF CONTENTS**

| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
| --- | --- | --- |
|  | List of Abbreviations  List of Figures  List of Tables  Abstract | iv  v  vi  vii |
| 1 | **INTRODUCTION** Introduction 1.2 Motivation for the work  1.3 [About Introduction to the project  including techniques]  1.5 Problem Statement  1.6 Objective of the work  1.7 Summary | 1  1  .2  2.  2. |
| 2 | **LITERATURE SURVEY**  2.1 Introduction  2.2 Core area of the project  2.3 Existing Models  2.3 Schuba and Spafford model  2.4 Observations  2.5 Summary | 12  12  13-14  14  14 |
| 3 | **SYSTEM ANALYSIS**  3.1 Introduction  3.2 Disadvantages/Limitations in the existing system  3.2.1 IP Spoofing  3.2.2 Path Addressing  3.2.3 Tiny Fragmentation  3.3 Proposed System  3.3.1 Tables  3.3.2 Chains  3.3.3 Targets  3.4 Summary | 15  15-16  16-17  17 |
| 4 | **SYSTEM DESIGN AND IMPLEMENTATION**  4.1 Introduction  4.2 Default configuration of the firewall  4.3 Setting rules to block certain IP’s  4.4. Conditional Testing  4.5 Summary | 18  18  19  19  20  20 |
| 5 | **PERFORMANCE ANALYSIS**  5.1Introduction  5.2 Performance Measures  5.3 Performance Analysis  5.4 Summary | 21  21-22  22-24  24 |
| 6 | **FUTURE ENHANCEMENT AND CONCLUSION**  6.1Introduction  6.2 Limitation/Constraints of the System  6.3 Future Enhancements  6.4 Conclusion | 25  25  25  25 |
|  | References | 26 |

**INTRODUCTION**

The need for secure data transmission is greater than ever before.Nowadays computer users resort to using VPN ’s and secure connection tools provided by Kaspersky and Norton, to ensure that they aren't been eavesdropped on and can transmit their data safely,without a man in the middle attack.These are employed by intranets and local area networks,consisting of closely connected computers known as nodes.

Hubs and switches enable data transmission and firewalls prevent unauthorised access,from external users and personnel,from the guarded network.Firewalls further monitor the data packets being sent from and being received by the network in question.Firewalls come in three main types-packet filtering,application and packet inspection.Here we will discuss about Packet filtering type of firewall.

Packet filtering firewalls can be broadly divided into two types-stateful and stateless.Stateful firewalls monitor the full state of active network connections and are constantly analyzing the complete context of traffic and data packets, seeking entry to a network. Once a certain kind of traffic has been approved by a stateful firewall, it is added to a state table and can travel more freely into the protected network. Traffic and data packets that don’t successfully complete the required handshake will be blocked.

Stateless firewalls are designed to protect networks based on information such as source and destination.Stateless firewalls filter packets based on the individual packets themselves.

To do so, stateless firewalls use packet filtering rules that specify certain match conditions. If match conditions are met, stateless firewall filters will then use a set of preapproved actions to guide packets into the network. If match conditions are not met, unidentified or malicious packets will be blocked.

Motivation-Our reason to strive for this project was to enrich our practical experience and knowledge in network security.Getting to work hands-on with security implementation and protection is surely the best way to learn.

**About our Project**

On Linux OS distributions,functionality is provided to users,to create a firewall of their own .For this purpose,a packet filtering framework called netfilters is made available,forming the bedrock of the firewall.Iptables is not a service or a package,in a Linux environment,but is an inbuilt tool,consisting of tables.These both combine to form a powerful firewall.On this framework,system users can set commands to accept or reject incoming traffic.Further rules can be set,to classify packets from each other, based on port number,protocol followed,ip address etc.

**Problem Statement**

Through our work,we want to find how users can benefit from having a firewall configured and set up,in order to repel network attacks.What are the benefits enjoyed by users and what else can be implemented on a system to form a solution towards safe networking.

**Objective of the work**

To demonstrate the working of a firewall,how it can be configured to meet the network administrator’s needs,to make the system and the connected network secure from unauthorized users

**Summary**

To implement a security device,which can aid safe networking between two isolated systems,with the interference of man in the middle attacks

**LITERATURE SURVEY**

**Introduction**

Data communications networks have become an infrastructure resource for businesses, corporations, government agencies, and academic institutions. Computer networking, however, is not without risks as Howard et al, illustrates in his analysis of over 92% of security incidents on the Internet between 2010 and 2020. Firewall technology is one mechanism to protect against network-based attack methods. A balanced approach to network protection draws from several other fields, such as physical security, personnel security, operations security, communication security, and social mechanisms. Classically, firewall technology has been applied to TCP/IP (transmission control protocol, internet protocol internetworks. Firewalls are used to guard and isolate connected segments of internetworks. “Inside” network domains are protected against “outside” untrusted networks, or parts of a network are protected against other.parts.To date there is neither a well designed reference model nor any theoretical background for firewall technology, let alone a definition of the term.

**Core Area of the Project**

Trablesi et al (2012) stated that firewalls control the access into and from the network based on a set of filtering rules, which reflect and enforce the organization’s security policy.

Nife et al (2020),states that for an efficient firewall implementation,it needs to have a well defined firewall policy,which all packets passing through the firewall have to respect.

Trablesi et al (2012) states that a TCP or UDP session is characterized by four attributes, namely the IP address of the client, the IP address of the server, the client port (known as source port), and the server port (known as destination port). Usually, the server port number allows us to identify the nature of the offered service.

**Existing Work**

We will discuss about one of the earliest firewall prototypes suggested by Christoph L. Schuba and Eugene H. Spafford

The reference model focuses on functionality required by firewall systems to enforce network domain security policies. For that reason we chose a functional model over other types of models, such as data processing, classification, stimulus-response, or process models. The idea is that systems are, at a conceptual level, composed of separate, interacting functional components. Our reference model can be interpreted as a system composed of several types of security components. The components are combined under certain constraints to make up a firewall system.

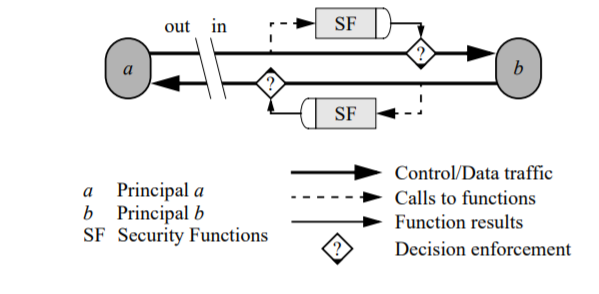


Figure 1-An abbreviated representation of the reference firewall model,as put forward by Christoph L. Schuba and Eugene H. Spafford

Consider the case where a principal ‘a’ outside of a protected network policy domain attempts to communicate with a principal ‘b’ inside that domain. Everything between the gap and the representation of principal ‘b’ is considered part of the protected network policy domain. All communications are divided into transmission units that are transmitted by the network. The reference model operates on one protocol layer or a range of protocol layers on transmission units at that layer (range, respectively). It operates on inbound as well as outbound communication traffic. The heavy, solid line represents the conceptual path that transmission units travel. Shaded boxes represent functions. In figure 1 the boxes labeled SF represent a collection of security functions that are applied to transmission units exchanged between principals ‘a’ and ‘b’. The dashed arrows represent the invocation of this collective function SF. Each SF receives portions or possibly even (a copy of) the entire transmission unit as input arguments. SFs calculate a result PASS or FAIL for each transmission unit. The diamond with the question mark ( ? ) represents the matching of the decision to its transmission unit and the decision branching and enforcement depending on the result. If the result is PASS, the transmission unit is forwarded to its destination; if the result is FAIL, an exception occurs (represented by the solid triangle in the diamond), and the transmission unit is dealt with accordingly (e.g., recorded to the audit log, and then discarded). The separation of SF into two boxes serves to further illustrate the bi-directionality of communications.

**Observations**

The model allows for unilateral and mutual authentication by choosing the appropriate authentication functions on inbound and outbound communication traffic and is a guide to structure firewall security services at a single layer or a range of layers in a layered model of computer networking.

The reference model does not impose a specific approach to the identification of communication traffic; rather it requires external naming, addressing, and directory mechanisms that may be used for name translation. The implementation of mechanisms is not addressed by the model.

**Summary**

We can infer from the model that it operates on communication traffic entering or leaving a network policy domain. It is implemented in layers on the OSI model. It therefore does not address the security problems associated with communication traffic that does not cross a domain’s perimeter, as is the case when insiders of an organization launch network based attacks against their own organization.Hence it cannot repel insider attacks or attacks caused by misuse of computer resources within the network or organization.

model operates on communication traffic entering or leaving a network policy domain. It therefore does not address the security problems associated with communication traffic that does not cross a domain’s perimeter, as is the case when insiders of an organization launch network based attacks against their own organization. Some mechanisms, however, are capable of protecting against such threats.

**SYSTEM ANALYSIS**

**Introduction**

In this section,we will discuss the merits and demerits of implementing a stateful firewall.The rationale for installing a firewall is almost always to protect a private network against intrusion. In most cases, the purpose of the firewall is to prevent unauthorized users from accessing computing resources on a private network, and often to prevent unnoticed and unauthorized export of proprietary information. In some cases, export of information is not considered important, but in many cases this is a major, though possibly unwarranted, concern. Many organizations will want to address the problem by not connecting to the Internet at all. This policy can be difficult to enforce. If the private network is loosely administered .An individual with a high speed dial-up modem or ethernet can quickly arrange an Internet SLIP connection that can compromise the security of an entire network

**Disadvantages/Limitations of the existing system**

As we discussed targets,we identified that ACCEPT was a vulnerable link to the firewall.It makes the firewall prone to attacks such as IP Spoofing, Path Addressing and Tiny Fragmentation.We will address each attack one by one

IP Spoofing Attack-Here, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. Because this occurs at the network level, there are no external signs of tampering.

Path Addressing Attack-In this attack,an attacker trying to infiltrate the target network,will send packets to the firewall,by planning the route of the packet as it travels to a computer within the network.

Tiny Fragmentation Attack-Packets consist of a port field and ip field among other fields.Networks such as Token Ring,Ethernet etc specify a limit to the size of the ip packet field.Firewalls reject those packets whose ip packet size is greater than the size specified.The attacker targets these rejected packets and fragment them into smaller packets and send them back to the firewall,which the firewall accepts.This is a vulnerability of the TCP Protocol,which is misused.

The other disadvantage is that stateful inspection firewalls cannot prevent application-layer attacks.The application layer,which is the 5’th layer of the OSI Model specifies the shared communications protocols and interface methods used by hosts in a communications network.

**Proposed System**

Here,we will provide a rundown of the various methods and terms that are essential,towards understanding the firewall and its configuration.

### Tables

As mentioned previously, tables allow you to do very specific things with packets. On modern Linux distributions, there are four tables:

The filter table: This is the default and perhaps the most widely used table. It is used to make decisions about whether a packet should be allowed to reach its destination.

The mangle table: This table allows you to alter packet headers in various ways, such as changing TTL values.

The nat table: This table allows you to route packets to different hosts on NAT (Network Address Translation) networks by changing the source and destination addresses of packets. It is often used to allow access to services that can’t be accessed directly, because they’re on a NAT network.

The raw table: iptables is a stateful firewall, which means that packets are inspected with respect to their “state”. (For example, a packet could be part of a new connection, or it could be part of an existing connection.) The raw table allows you to work with packets before the kernel starts tracking its state. In addition, you can also exempt certain packets from the state-tracking machinery.

### 

### 

### Chains

Now, each of these tables are composed of a few default chains. These chains allow you to filter packets at various points. The list of chains iptables provides are:-

The INPUT chain: The INPUT chain rules apply to packets that are incoming to our system,which is the destination point.Packets are checked if they align with the rules This chain is present in the mangle and filter tables.

The OUTPUT chain: The rules here apply to packets that are outgoing from a system.If rules are followed,then the packets go to the specified destination computer,with help of it;s IP Address.This chain is present in the raw, mangle, nat and filter tables.

The FORWARD chain: The rules here apply to any packets that are routed through the current host.Here,packets first have to pass through the FORWARD chain,before being allowed to route. This chain is only present in the mangle and filter tables.

**Targets**

Decisions that are taken by the firewall to incoming,outgoing and routing packets are called targets.Targets are specified by the network administrator configuring the firewall.There are mainly three rules:-

ACCEPT: This causes iptables to accept the packet.

DROP:This rule,once enforced,causes the iptables to drop the packets.For users trying to send packets to your system,no message is given that the packets have been rejected.

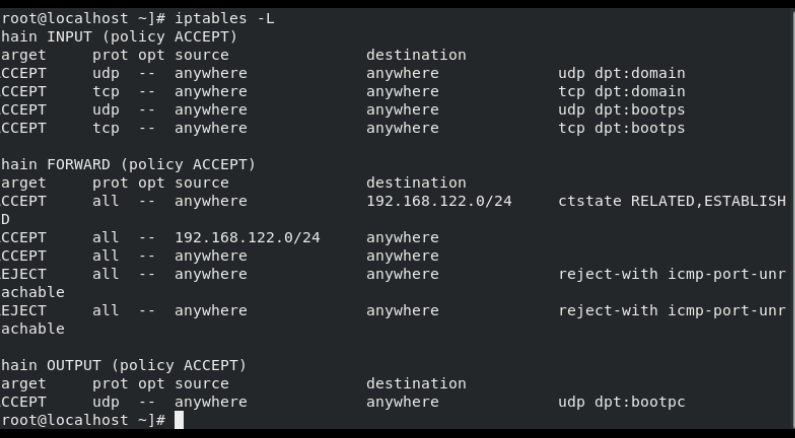
REJECT: Here the iptables rejects the packet. It sends a “connection reset” packet in case of TCP, or a “destination host unreachable” packet in case of UDP or ICMP.The user sending packets is served with a message that the packets that they have sent are rejected by the destination system.

In summary,we have discussed the various factors that go into creating the prototype

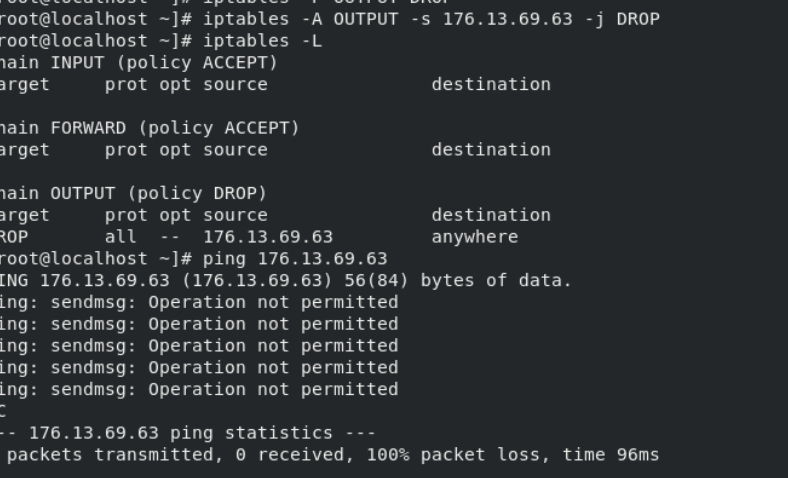
**SYSTEM DESIGN AND IMPLEMENTATION**

**Introduction**

The proposed firewall is implemented on CentOS distribution of Linux.Here the .iso file of the Linux OS is installed on VirtualBox.The bedrock of our firewall is based on a packet filtering framework named iptables. It allows you to allow, drop and modify traffic leaving in and out of a system. A tool, iptables builds upon this functionality to provide a powerful firewall, which you can configure by adding rules.

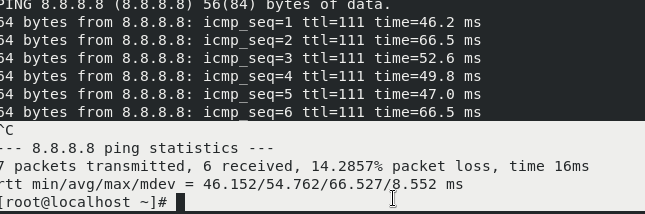
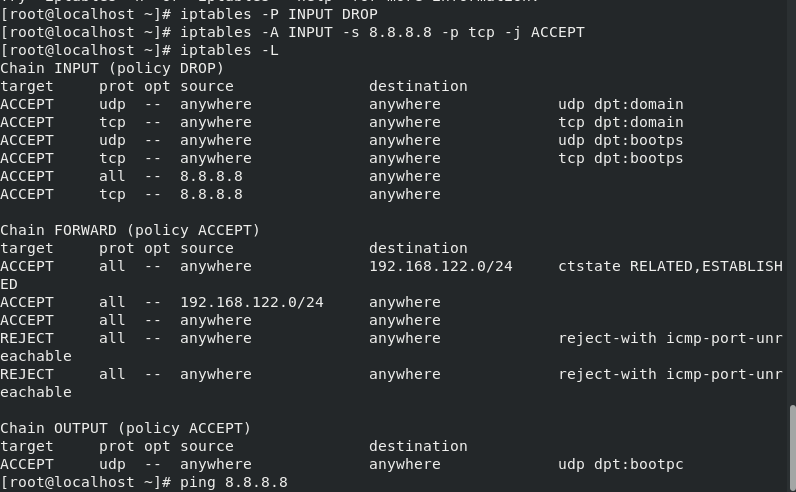
 Figure-2 We check what the iptables rules are,at after system boot.It shows that the chains (INPUT,OUTPUT and FORWARD) have default target ACCEPT.

From command line,we first check if firewalld service is running,From the figure,we see that no protocol has been specified yet.Source and Destination IP fields are set to anywhere and no optional conditions are set

Figure 3 Blocking packets from out system,after setting target of OUTPUT policy as DROP.Packets aren’t able to be transmitted,after pinging

Here,we initially set the OUTPUT policy to DROP,by using the command iptables -L OUTPUT DROP.This means that,by default no packets can’t be transmitted from our system.Unless the administrator/root user configures the OUTPUT policy’s target back to ACCEPT.

After setting the command configuration,the changes are respectively reflected in the iptables,for the user to view.A 100 % packet loss is subsequently recorded on the host system.

Condition Testing-Will the firewall accept packets even if policy is set to DROP? Figures 4 and 5-The user has set a rule to accept packets following tcp protocol into the system,while switching target of INPUT policy to DROP

After the rule was set,we pinged the ip address 8.8.8.8 in order to check if packets would get accepted or rejected.We observed that packets were accepted and transmitted both ways,but faced a packet loss of 14.28% (meaning one packet failed to be received).The whole transmission took 16ms to execute.

In short,we have implemented the rules that can allow a firewall to function properly.The firewall and the packets follow the enforced rules.For an efficient firewall to function,it needs to have a good security policy.

**PERFORMANCE ANALYSIS**

Using the built prototype,we tested both acceptance and denial of packets from certain ip’s,protocols and ports,on four different systems.10 observational instances were recorded and it’s average is taken as the percentage.The results are given below:-

**IP Addresses (Average % of 10 observations)**

| **System** | **Acceptance Rate(in %)** | **Block Rate (in %)** |
| --- | --- | --- |
| **1** | **99.2** | **100** |
| **2** | **99.5** | **100** |
| **3** | **100** | **98** |
| **4** | **100** | **95** |

Table 1- Packets incoming and outgoing from system,based on ip address rules,placed on INPUT and OUTPUT chains

**Protocols (Average % of 10 observations)**

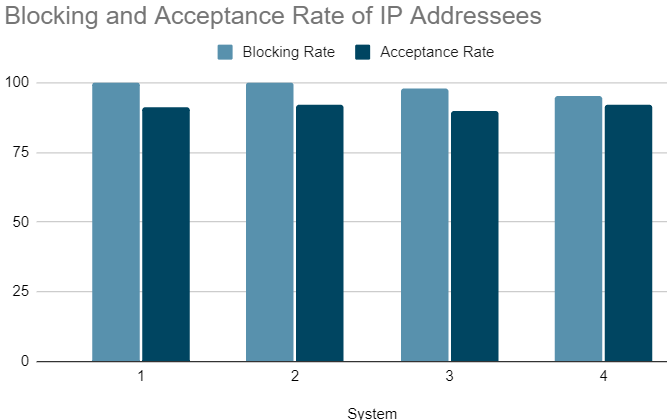
| **System** | **Acceptance Rate(in %)** | **Block Rate (in %)** |
| --- | --- | --- |
| **1** | **98** | **100** |
| **2** | **100** | **100** |
| **3** | **97** | **100** |
| **4** | **100** | **100** |

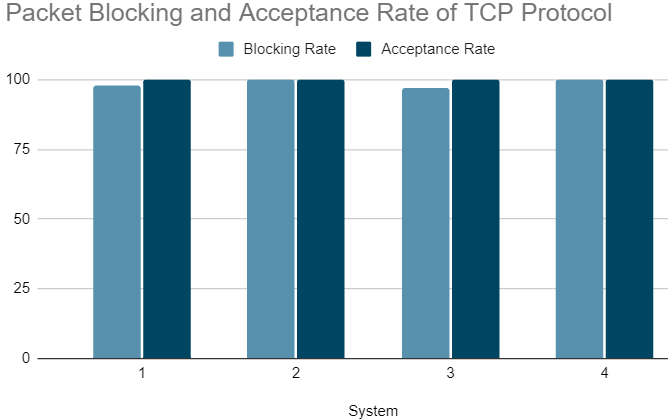
Table 2-Packets incoming and outgoing from system,based on tcp protocols rules,placed on INPUT and OUTPUT chains

| **System** | **Packets Sent** | **Throughput** |
| --- | --- | --- |
| **1** | **10** | **0.462** |
| **2** | **10** | **0.435** |
| **3** | **10** | **0.429** |
| **4** | **10** | **0.449** |

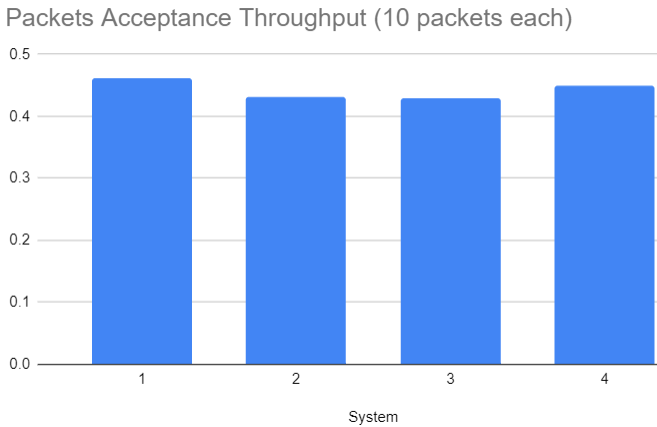
Table 3-Throughput of packets incoming and outgoing from system

**Graph Representation of Observations**

**** Graph 1-Bar chart representing effectiveness of the SI firewall handling IP based packet transmissions

****

Graph 2-Bar chart representing effectiveness of the SI firewall handling TCP targeted packets incoming and outgoing from the system

 Graph 3-Representation of packet transmission throughput (Packets/Time)

**Summary**

From the graphs and tables we observe that the firewall prototype,is efficient in filtering required packets from the unwanted and is able to enforce rules strictly upon both incoming and outgoing packets,provided that the user has specified the rules correctly

**FUTURE ENHANCEMENT AND CONCLUSION**

Firewalls are considered an essential part of any information security system. They are the first defense line against any cyber attack. In this paper, we presented an assessment methodology to analyze the performance of different firewalls platforms. The performance analysis considered throughput, and incoming and outgoing rates.

When developing a stateful inspection firewall,we have to keep in mind that it is ill-equipped to handle certain limitations,once configured and implemented. These limitations consist of, firstly, "Shadowed rules" (the rule that cannot match with any packet because a packet will be matched with other rules above) which can lead to security problems. Secondly, limitations about swapping positions between rules can bring a change in firewall policy and cause security problem.Packet filters do not filter fragmented packets well and are stateless; they do not maintain any state information for added protection.

Research firms and tech pundits have predicted the demise of the firewall,for years now, chiefly because it doesn’t protect against modern day threats and is often so mismanaged it causes more problems than it solves.On network based firewalls,today’s applications live in hybrid environments (public and private cloud resources).That means the firewall can't see what's going on, where the connections are coming from, or where they're going, while the IP addresses change all the time or are hidden.

The biggest change over the last few years has been the rise and dominance of the “next gen” firewall.They are an advanced version of the traditional firewall that doesn’t merely block ports and IPs, NGFWs feature much smarter technology, combining IDS, anti-spam and more, offering a full spectrum of defense. They’re also “application aware” and much better suited to today’s app-centric world.

In conclusion, we can state that firewalls are not a thing of the past.Each one comes with thor own set of merits and demerits.More innovative technologies are emerging from the field of network security such as the afore-mentioned NGFW and UTM (Unified Threat Management) firewalls,which lead the way for safe networking in the future

**REFERENCES**

1 Christoph L.Schuba and Eugene H.Spafford, A Reference Model for Firewall Technology (1997)

2 Fahad N. Nife & Zbigniew Kotulski, Application-Aware Firewall Mechanism for Software Defined Networks,2020605–626(2020)

3 Zouhir Trablesi, Teaching Stateless and Stateful Firewall Packet Filtering: A Hands-on Approach, (2012)

4 Leslie .F Sekos, Packet analysis for network forensics:A comprehensive survey,[Volume 32](https://www.sciencedirect.com/science/journal/26662817/32/supp/C), March 2020, 200892

5 Thawatchai Chomsiri,Xiangjian He,Priyadarsi Nanda, Limitation of Listed-Rule Firewall and the Design of Tree-Rule Firewall (2012)

6 Yordanos Beyene,Michalis Faloutsos,Harsha V. Madhyastha, SyFi: A Systematic Approach for Estimating Stateful Firewall Performance (2012)