Spring 2014

A Federated Architecture for Heuristics Packet Filtering in Cloud Networks

Ibrahim M. Waziri Jr

A FEDERATED ARCHITECTURE FOR HEURISTICS PACKET FILTERING IN CLOUD NETWORKS

by

IBRAHIM WAZIRI JR

(Under the Direction of Jordan Shropshire)

ABSTRACT

The rapid expansion in networking has provided tremendous opportunities to access an unparalleled amount of information. Everyone connects to a network to gain access and to share this information. However when someone connects to a public network, his private network and information becomes vulnerable to hackers and all kinds of security threats. Today, all networks needs to be secured, and one of the best security policies is firewall implementation.

Firewalls can be hardware or cloud based. Hardware based firewalls offer the advantage of faster response time, whereas cloud based firewalls are more flexible. In reality the best form of firewall protection is the combination of both hardware and cloud firewall.

In this thesis, we implemented and configured a federated architecture using both firewalls, the Cisco ASA 5510 and Vyatta VC6.6 Cloud Based Firewall. Performance evaluation of both firewalls were conducted and analyzed based on two scenarios; spike and endurance test. Throughputs were also compared, along with some mathematical calculations using statistics. Different forms of packets were sent using a specialized tool designed for load testing known as JMeter.

After collecting the results and analyzing it thoroughly, this thesis is concluded by presenting a heuristics method on how packet filtering would fall back to the cloud based firewall when the hardware based firewall becomes stressed and over loaded, thus allowing efficient packet flow and optimized performance.

The result of this thesis can be used by Information Security Analyst, students, organizations and IT experts to have an idea on how to implement a secured network architecture to protect digital information.

INDEX WORDS: Cloud Networks, Cloud Firewalls, Cloud Security, Hardware Firewalls, Packet Filtering, Packet Classification, Network Security

A FEDERATED ARCHITECTURE FOR HEURISTICS PACKET FILTERING IN CLOUD NETWORKS

by

IBRAHIM WAZIRI JR

B.Sc. in Electrical & Electronics Engineering Technology

(Telecommunications), 2009.

A Thesis Submitted to the Graduate Faculty of Georgia Southern University in

Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

STATESBORO, GEORGIA

2014

A FEDERATED ARCHITECTURE FOR HEURISTICS PACKET FILTERING IN CLOUD NETWORKS

by

IBRAHIM WAZIRI JR

Major Professor: Jordan Shropshire, Ph.D.
Committee: Chris Kadlec, Ph.D.
Timur Mirzoev, Ph.D.

Electronic Version Approved:
Spring 2014

DEDICATION

To Dad...

ACKNOWLEDGEMENTS

The successful and satisfactorily completion of this thesis would never be possible without the guidance and support of my professor Dr. Jordan Shropshire. I would like to express my immense gratitude to him for his constant guidance, moral support and motivation which made a great impact in my life. I am truly grateful for the opportunity you gave me. Thank you!

I would like to thank Dr. Chris Kadlec and Dr. Timur Mirzoev for all the advice and taking time to review my thesis and make suggestions for its improvement.

My appreciations to my friends that helped me with setting up the standalone computers used in this thesis.

My appreciation also goes to the professors whom took the time to teach me here at Georgia Southern and the entire faculty members and staff of the Information Technology Department.

I would also like to thank my family members for the enormous support and my friends for taking me along on this incredible journey.

Lastly, my gratitude to all the people who helped me here at Georgia Southern, without you none of these would be possible.

Thank you all...

Yours truly,

Ibrahim Waziri Jr.

ACRONYMS

ACL	Access Control List
ACM	Association for Computing Machinery
ASA	Adaptive Security Appliance
ContH	Continue on Hardware
CPU	Central Processing Unit
CPUU	CPU Utilization
CSA	Cloud Security Alliance
DLP	Data Leakage Prevention
DoS	Denial of Service
FTP	File Transfer Protocol
GB	Gigabyte
GUI	Graphical User Interface
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
I/O	Input / Output
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPAM	IP Address Management
IPS	Intrusion Prevention Systems
IT	Information Technology
JVM	Java Virtual Machine
LAN	Local Area Network
MAN	Metropolitan Area Network
MemU	Memory Utilization
MgC	Migrate to Cloud
NAT	Network Address Translation

NIC	Network Interface Card
NSTISSC	National Security Telecommunications and Information Systems Security Committee
OS	Operating System
PaaS	Platform as a Service
PC	Personal Computer
Pd	Packet Drop
RAM	Random Access Memory
SaaS	Software as a Service
Scen1	Scenario 1
SLA	Service Level Agreement
St.Dev	Standard Deviation
SVR	Security Virtual Appliances
TB	Terabyte
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
Tp	Throughput
VM	Virtual Machine
VMM	Virtual Machine Monitor
vNIC	Virtual Network Interface Card
VPN	Virtual Private Network
VSR	Virtual Software Router
vSwitch	Virtual Switch
WAN	Wide Area Network

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SCREEN SHOTS

CHAPTER ONE
INTRODUCTION

1.1 Introduction

Information and data sharing through connectivity has become an important factor in our daily lives. Individuals, small and big enterprises are all desperate for a sharing medium that could be used to reach another point with just a click. Thanks to networking, it has delivered that need. Today the Internet has revolutionized the computer and communication world like nothing before. The internet is now a worldwide broadcasting medium, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location.

The Internet connects the world just like highways connect cities. It is an electronic information superhighway which connects schools, businesses, homes, universities and organizations. It provides researchers and business leaders with opportunities that seemed like science fiction not more than a decade ago. Unlike our traditional highway where we have full control of our vehicles while driving, in the internet there is limited control to information when it gets out there. Considering that everyone can connect to the internet, which possesses a lot of security threats to everyone trying to secure their information.

As a result of this, the study of information security came about. In recent years information security has become a more important issue for most large companies around the world (Nakrem 2007).

1.2 Information Security

Information security is commonly thought as a process and not a product (Tetteywayo and Akpabi 2007). Information security has become the major concern of every enterprise. It is crucial to apply all security majors to protect data on their networks.

The U.S National Information Systems Security Glossary defines "Information Systems Security" as:

"*the protection of Information systems against unauthorized access to or modification of information, whether in storage, processing or transmit, and against the denial of service authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats"* (NSTISSC 2000).

They also state that the widely accepted elements of information security (mnemonic – "CIA') are:

- Confidentiality
- Integrity
- Availability (NSTISSC 2000).

For enterprises and individuals to better secure their information, they need to implement a security measure one of which is a firewall. A firewall is one of the core components of a network security implementation (Tetteywayo and Akpabi 2007). A further discussion on what a firewall is how it works and how it is being deployed will be explained in a later chapter.

1.3 Problem Statement

Securing a cloud network in a virtualized environment can sometimes be tough, a user cannot access hardware resources the service provider is rendering. One cannot dedicate a hardware firewall for a cloud network, so deciding which type of firewall to use to ensure the security of information on the cloud arises. Using cloud-based firewalls such as Vyatta is considered important.

With different types of network firewalls available, deciding on the best firewall implementation can be a problem. With each type of firewall either hardware or cloud-based having its advantages and disadvantages, deployment decision is based on type of network and security requirements. Debates and research have been conducted on which firewall is better. Software firewalls are known with the advantage of ease of use due to GUI for configuration, but one of its disadvantage is it provides less security. Considering it is installed on an OS, an attacker may be able to hack the firewall itself. Hardware firewalls are known to provide great performance considering they have no operating system or minimal operating systems, and they can handle greater amount of traffic, but some of their disadvantage is that they are expensive and are less upgradable. As a result of these differences, it is agreed that deployment of both Hardware and Cloud based firewalls provides better performance and security in a network.

In this thesis, we address the problem that could lead to a total failure of a network when hardware based firewall fails, or becomes non-responsive. We design an architecture and present heuristics rules that will allow all services to migrate to a cloud based firewall when the hardware firewall fails.

1.4 Research Objectives

Objective 1: Assess the performance of hardware-based firewalls in cloud networks.

Objective 2: Assess the performance of cloud-based firewalls in cloud networks.

Objective 3: Assess the performance of federated firewalls architecture in cloud networks.

Objective 4: Design an integrated firewall architecture with a fallback logic for cloud networks

1.5 Purpose and scope of study

This thesis sought to provide information/network security engineers, students and organizations with architecture for the best packet filtering technique in a federated firewall network. The study identifies the performance of different types of firewalls in a network.

Given the fact that Cisco ASA is the most common firewall appliance in networks and Vyatta is a well-known cloud-based firewall motivated the choice of using these devices.

The proposed architecture would be such that both firewalls would work hand in hand to provide the best security in cloud networks. The research was conducted in a laboratory using hardware and virtualized resources. The study presented will provide security educators and students the opportunity on how to implement firewalls. All this would be possible in the virtualized environment.

The reasons behind the study were:

- To understand what Information Security is within a Cloud Network.

- To understand security issues and to provide the appropriate security technique that is being used in today's Cloud Computing world
- To identify the best security practice in Cloud Networks
- To suggest some counter measures faced in firewall deployments within a Cloud Network.
- To provide a pattern for optimized packet filtering in Cloud Networks.

1.6 Delimitations

This research aims at implementing a network architecture that uses two types of firewalls; hardware based and cloud based firewalls. There are different types of firewalls available, but for the purpose of this work we limited our choice to only Cisco ASA 5510 as the hardware based firewall, and Vyatta VC6.6 as the cloud based firewall. This research also presents heuristic rules that will allow migration of packet filtering services from a hardware based to a cloud based firewall when the hardware based firewall fails in a network. Regarding the choice of the webserver, we have limited the study to building an Apache webserver inside an Ubuntu 12.04 Linux distribution. Throughout this study, we used an ESXi 5.0 hypervisor, and all VM's are 64bit Windows 7 OS. We used a load testing tool known as JMeter to generate and send legitimate HTTP packets to the target. And the result of this study is limited to two scenarios; spike and endurance test. Throughput and mathematically calculations using statistics are also compared. Resources and in-depth analysis of the devices used in the research are outlined in later chapters.

1.7 Thesis Structure

This thesis is structured into seven chapters:

- Chapter 1 discusses a brief introduction about Information Security, the thesis problem statement, research questions, and the scope of the work.
- Chapter 2 discusses the background of Networking, Cloud Computing, Firewalls and security aspects of Networks & Cloud Computing.
- Chapter 3 presents the process of literature review and related findings.
- Chapter 4 presents the methodology used in this study.
- Chapter 5 discusses how the study and test are implemented, and the required resources used to conduct this study.
- Chapter 6 the test results are collected and analyzed.
- Chapter 7 discusses the result, drawn conclusion and recommended areas for future work.

A visualized thesis structure is presented in the figure 1 below:

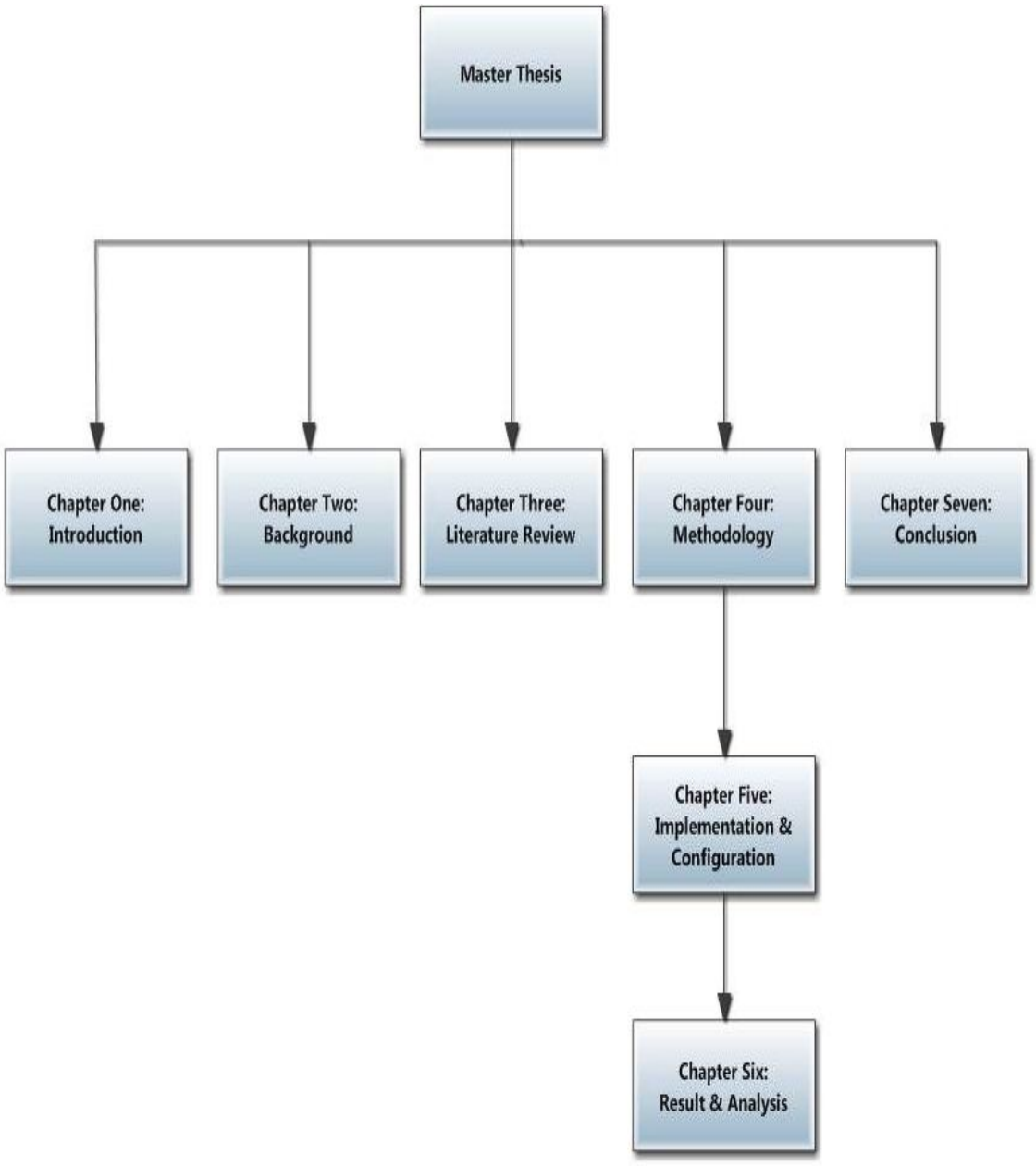


Figure 1: Thesis Structure

CHAPTER TWO
BACKGROUND

2.1 Basics of Data Communication & Networking

When we communicate, we are sharing information. This sharing of information can be between individuals, usually face to face, or remote communication which takes place over distance. The term telecommunication, which includes television, telegraphy, telephony etc., means communication at a distance (Forouzan 2003).

The word data refers to facts, concepts, and instructions presented in whatever form is agreed upon by the parties creating and using the data.

"*In computer information systems, data are represented by binary information units (or bits) produced and consumed in the form of 0s and 1s*" (Forouzan 2003).

2.1.1 Data communication

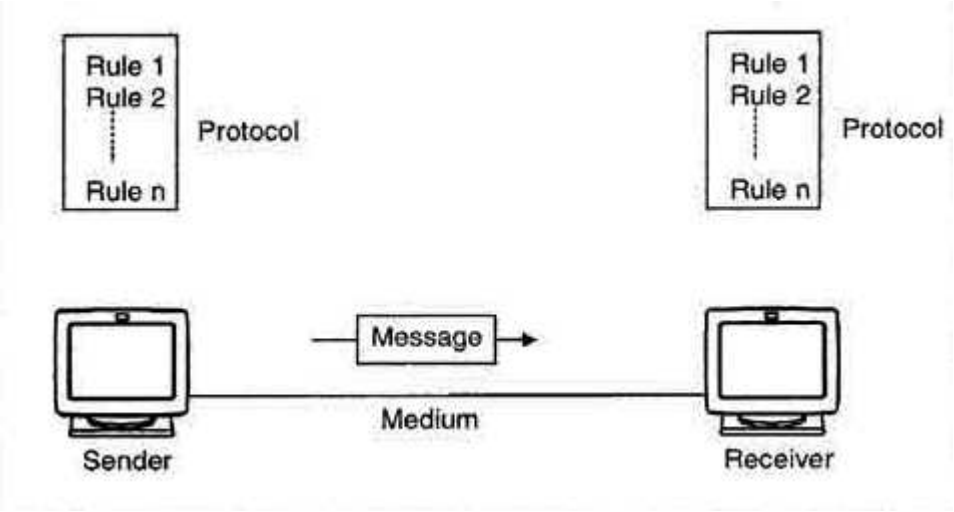
Data communication is the exchange of data (in the form of 0s and 1s) between two devices via some form of transmission medium such as a wire cable. Usually the communication is considered local if the communicating devices are in the same building or a similarly restricted geographical area; the communication is remote if the devices are farther apart.

For data communication to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communication system depends on three fundamental characteristics:

- Delivery – The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
- Accuracy – The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
- Timeliness – The system must deliver data in a timely manner. Data delivered late are useless. In the case of video, audio, and voice data, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

Data communication components

A data communication system has five components (Forouzan 2003) see figure 2 below:



Source: ecomputernotes.com

Figure 2: Data Communication Components

1. Message: The message is the information (data) to be communicated. It can consist of text, numbers, pictures, sound or video – or any combination of these.

2. Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera and so on.
3. Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television and so on.
4. Medium: The transmission medium is the physical path by which a message travels from sender to receiver. It can be a twisted-pair cable, co-axial cable, fiber-optic cable, laser, or radio waves.
5. Protocol: A protocol is a set of rules that governs data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating; just as a person speaking Spanish cannot be understood by a person speaking Japanese.

2.1.2 Networks

A network is two or more computers connected together to share resources such as files or a printer. For a network to function, it requires a network service to share or access a common medium or pathway to connect the computers. To bring it all together, protocols give the entire system common communication rules (Regan 2004).

Source: cksolutions.ie

Figure 3: Computer Network

Network Protocols

In computer networks, communication occurs between anything capable of sending and receiving information in different systems. An example includes application programs, file transfer packages, browsers, database management systems, and electronic mail software. A system is a physical object like computer.

Two computers cannot just send bit streams (0s and 1s) and expect to be understood. For communication to occur the system must agree on a protocol. A definition of protocol is stated above and a full detail of how protocols work is outside the scope of this thesis.

Types of Networks

Today, networks are broken into three main categories: a Local Area Network (LAN), a Metropolitan Area Network (MAN) and a Wide Area Network (WAN).

The category a network falls into is determined by its size, its ownership, the distance it covers, and its physical architecture.

Local Area Network

A LAN is a privately owned network that links the devices in a single office, building, or campus (see Figure 4 below). Depending on the needs and type of technology used, a LAN can be as simple as two PC's and a printer in someone's home or office, or it can extend through a company and include voice, sound and peripherals. Currently, LAN size is limited to a couple of miles.

Source: hill associates (hill2dot0.com)

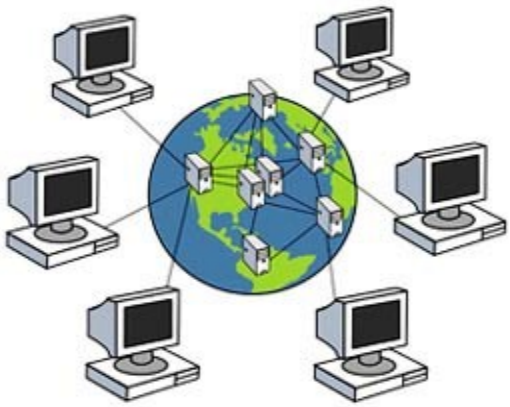
Figure 4: LAN

Metropolitan Area Network

MAN is designed to extend over an entire city. It may be a single network such as a cable television network, or it may be a means of connecting a number of LAN's into a larger network so that resources may be shared LAN-to-LAN as well as device-to-device.

Wide Area Network

WAN provides long-distance transmission of information over large geographical areas that may comprise a country, a continent, or even the whole world.



Source: Computer Network Solutions (computernetworks.com)

Figure 5: WAN

Internetworks

When two or more networks are connected, they become an internetwork, or widely known as the Internet.

2.2 Basics of Cloud Computing

The National Institute of Standards and Technology NIST defined Cloud Computing as "*A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g.., networks, servers, storages, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*." (Mell and Grance 2011).

In a nutshell, cloud computing is a way of separating an application from the operating system and hardware that runs everything.

Also the Cloud Security Alliance (CSA) defined cloud computing as "*an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them"* (CSA 2009).

Cloud Computing is composed of characteristics, service and deployment models (Mell and Grance 2011). Each of these will be discussed in-depth in the following sub chapters.

2.2.1 Cloud Computing Characteristics

1. On-demand self-service: a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2. Broad network access: capabilities are available over the network and accessed through standard mechanism that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops and workstations).
3. Resources pooling: the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but they may be able to specify location at a higher level of abstraction e.g., country, state, or datacenter. Examples of resources include storage, processing, memory, and network bandwidth.
4. Rapid elasticity: capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensuration with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriate in any quantity at any time.
5. Measured service: cloud systems automatically control and optimize resources use by leveraging a metering capability, at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resources usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

2.2.2 Cloud Computing Service Delivery Models

There are 3 delivery service models in cloud computing, which are:

Software as a Service (SaaS):

In SaaS capabilities provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Applications reside on the top of the cloud stack. Services provided by this layer can be accessed by end users through web portals. Therefore, consumers are increasingly shifting from locally installed computer programs to on-line software services that offer the same functionality. Traditional desktop applications such as word processing and spreadsheet can now be accessed as a service in the web. This model of delivering applications, SaaS, alleviates the burden of software maintenance for customers and simplifies development and testing for providers.

Platform as a service (PaaS):

In PaaS capabilities provided to the consumer is deployed onto the cloud infrastructure. Consumers use acquired applications created using programming languages, libraries, services, and the tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including the network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

In addition to infrastructure-oriented clouds that provide raw computing and storage services. Another approach is to offer a higher level of abstraction to make a cloud easily programmable. A cloud platform offers an environment on which developers create and deploy applications and do not necessarily need to know how many processors or how much memory that applications will be using. In addition, multiple programming models and specialized services (e.g., data access, authentication, and payments) are offered as building blocks to new applications.

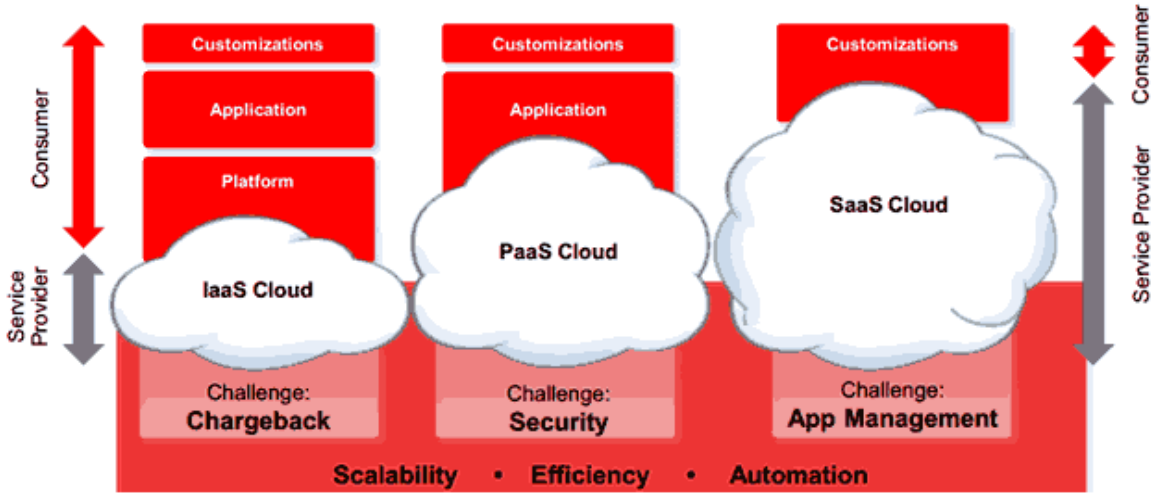
Google AppEngine, an example of PaaS offers a scalable environment for developing and hosting web applications, which are written using specific programming languages such as Python or Java. Building blocks include an in-memory object cache (memcache), mail service, instant messaging service (XMPP), an image manipulation service, and integration with Google Accounts authentication service.

Infrastructure as a Service (IaaS)

In IaaS capabilities provided to the consumer is provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which includes operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of selected networking components (e.g., host firewalls).

Offering virtualized resources (computation, storage, and communication) on demand is known as IaaS. This cloud infrastructure enables on-demand provisioning of servers running several choices of operating systems and a customized software stack. Infrastructure services are considered to be the bottom layer of cloud computing systems.

Amazon Web Services mainly offers IaaS, which in the case of its EC2 service offers VMs with a software stack that can be customized similar to how an ordinary physical server would be customized. Users are given privileges to perform numerous activities to the server, such as: starting and stopping it, customizing it by installing software packages, attaching virtual disks to it, and configuring access permissions and firewalls rules.



Source: crmsearch.com

Figure 6: IaaS, PaaS and SaaS

2.2.3 Cloud Computing Deployment Models

Private Cloud:

This cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community Cloud:

This cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud:

This cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid Cloud:

This cloud infrastructure is a composition of two or more distinct cloud infrastructure's (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

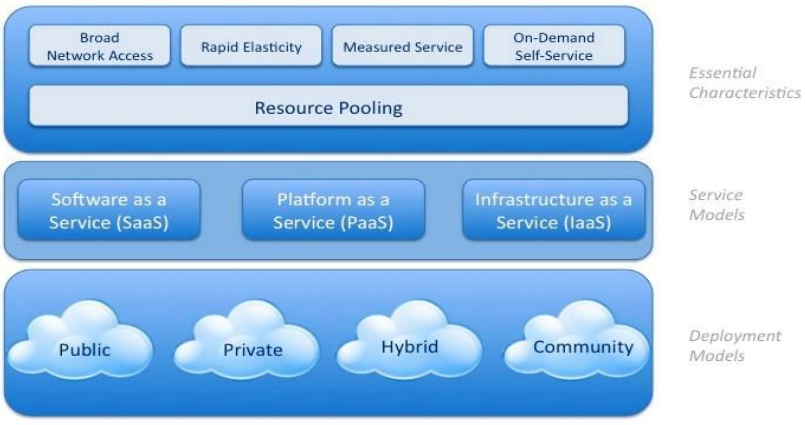


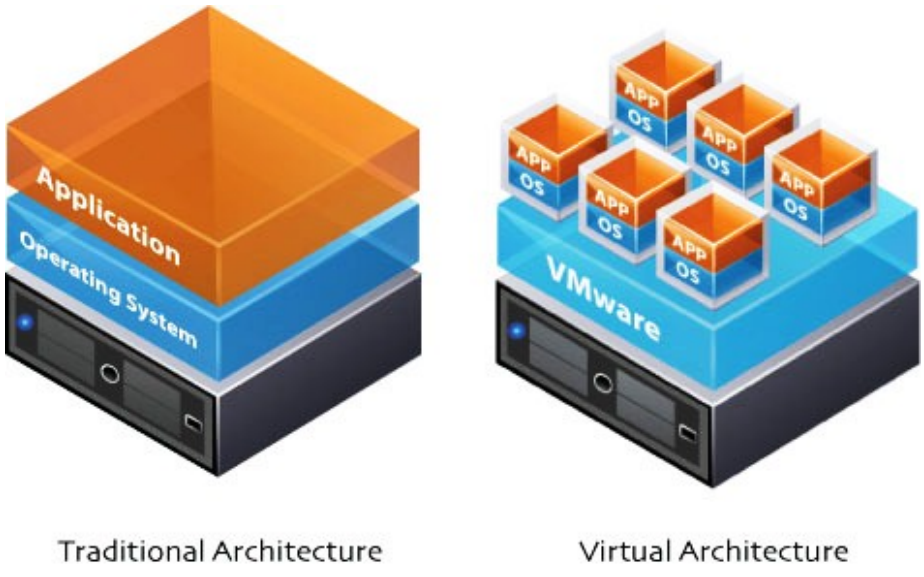
Figure 7: Cloud Computing Deployment Models (CSA 2009).

2.2.4 Virtualization

Cloud Computing services are usually backed by large-scale data centers composed of thousands of computers. Such data centers are built to serve many users and host many disparate applications. For this purpose, hardware virtualization can be considered as a perfect fit to overcome most operational issues of data center building maintenance.

The idea of virtualizing a computer system's resources, including processors, memory, and I/O devices, has been well established for decades, aiming at improving sharing and utilization of computer systems (Buyya, et al 2011). Virtualization allows running multiple operating systems and software stacks on a single physical platform.

The figure below shows a software layer, the hypervisor also known as a virtual machine monitor (VMM), which mediates access to the physical hardware presenting to each guest operating system (VM) is a set of virtual platform interfaces.



Source: vmware.com

Figure 8: Traditional & Virtual Architecture

Virtualization has been a key enabling technology for the evolution of cloud computing into its current form. In particular, a hardware virtualization has enabled IaaS providers to efficiently use the available hardware resources in order to provide computing and storage services to their clients.

2.2.5 Virtual machine

A virtual machine is an operating system or an environment created using a virtual machine monitor (hypervisor) (Popek 1974). A virtual machine is taken to be an efficient, isolated duplicate of the real machine. A better understanding of what a virtual machine is explained in 2.2.6 below.

2.2.6 Virtual Machine Monitor (VMM)

Also known as a hypervisor is a software for computing system that creates efficient, isolated programming environments (virtual machines) that are duplicates which provides user with the appearance of direct access to the real machine environment (Robin & Irvine 2000).

A hypervisor allows multiple operating-systems (VM's) to run concurrently on a single hardware platform. There are two different types of VMM's that can create a virtual machine environment. These types are referred to as Type I and Type II (Robin & Irvine 2000).

2.2.7 Types of VMM

Type I VMM

Type I VMM also known as a bare-metal runs on a bare machine. It is an operating system with virtualization mechanisms.

A type I VMM runs directly on the machine hardware. It is an operating system or kernel that has mechanisms to support virtual machines. It performs scheduling and resources allocation for all virtual machines in the system and requires drivers for hardware peripherals.

Figure 9: Type I VMM

Type II VMM

A type II VMM runs as an application on a host operating system and relies on the host OS for memory management, processing scheduling, resource allocation and hardware drivers. It only provides virtualization support services. The operating system that controls the real hardware is called the "host OS" the host OS does not need or use any part of the virtualization environment. Every OS that is run in the Type II virtual environment is called a guest OS.

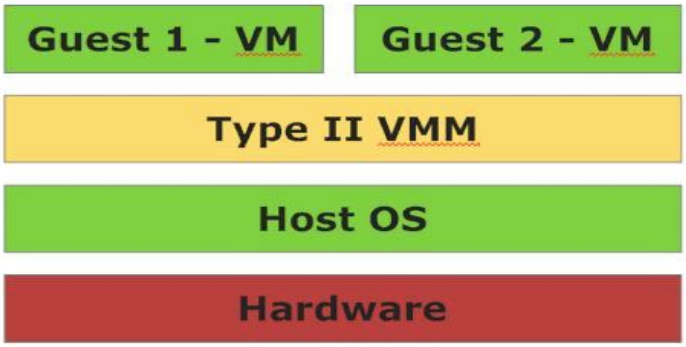


Figure 10: Type II VMM

2.2.8 VMM Platforms

A number of VMM platforms that are the basis of many utility or cloud computing environments exist. The most notable ones are: VMware ESXi, Xen, and KVM. All of these are outlined in the following sections.

VMware ESXi:

VMware is a pioneer in the virtualization market. Its ecosystem of tools ranges from server and desktop virtualization to high-level management tools. ESXi is the VMM from VMware. It is a bare-metal hypervisor, meaning that it installs directly on the physical server, whereas others may require a host operating system. It provides advanced virtualization techniques of processor, memory, and I/O. Especially, through memory ballooning and page sharing. It can overcommit memory, thus increasing the density of VMs inside a single physical server.

Xen:

The Xen hypervisor started as an open-source project and has served as a base to other virtualization products, both commercial and open-source. It has pioneered the para-

virtualization concept, in which the guest operating system by a means of a specialized kernel can interact with the hypervisor, thus significantly improving performance. In addition to an open-source distribution, Xen currently forms the base of commercial hypervisors of a number of vendors, most notably Citrix Xen Server and Oracle VM.

KVM:

The kernel-based virtual machine (KVM) is a Linux virtualization subsystem. Is has been part of the mainline Linux kernel since version 2.6.20, thus being natively supported by several distributions. In addition, activities such as memory management and scheduling are carried out by existing kernel features, thus making KVM simpler and smaller than hypervisors that take control of the entire machine. KVM leverages hardware-assisted virtualization, which improves performance and allows it to support unmodified guest operating systems. Currently, it supports several versions of Windows, Linux, and UNIX.

2.3 Security aspects of Networks & Cloud Computing

2.3.1 Network Security

According to Cisco: “Network Security refers to any activity designed to protect a network. Specifically, these activities protect the usability, reliability, integrity and safety of a network and data. Effective network security targets a variety of threats and stops them from entering or spreading on a network” (Cisco 2014).

Network Security Threats:

Many security threats today are spread over the internet. The most common include:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft etc.

Network Security Components:

No single solution protects you from a variety the threats. One needs multiple layers of security. If one fails, others still stand. Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect you from emerging threats.

A network security system usually consists of many components. Ideally all components work together, which minimizes maintenance and improves security.

Network security components often include:

- Anti-virus and anti-spyware
- Firewall, to block unauthorized access to your network
- Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks

- Virtual Private Networks (VPNs), to provide secure remote access.

2.3.2 Cloud Security

Cloud computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Customers are both excited and nervous at the prospects of Cloud Computing. They are excited by the opportunities to reduce capital costs. They are excited for a chance to divest them of infrastructure management, and focus on core competencies. Most of all, they are excited by the agility offered by the on-demand provisioning of computing and the ability to align information technology with business strategies and needs more readily. However, customers are also very concerned about the risks of Cloud Computing if not properly secured. And also the loss of direct control over systems for which they are nonetheless accountable.

Security controls in cloud computing are for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions.

Some of the security threats to cloud computing outlined by Cloud Security Alliance (CSA) are mentioned below (CSA 2010).

Cloud Security Threats:

- Abuse and nefarious use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insider

- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

In later chapters we would discuss the security issues on each Cloud computing service models, and a possible solution to each.

2.4 Firewalls

2.4.1 Definitions of Firewall

The internet is an exciting and wonderful place to browse and explore. It is the great frontier and another grandiose achievement of mankind. In reality the World Wide Web is merely a collection of routers and servers that make up the largest wide-area network (WAN) in recorded history. The collection of networking gears provides mail servers, websites and other information storage and retrieval systems which are all connected to the Internet to be accessible to every person who is also connected. It has even been said that the Internet contains a collective institutional knowledge of mankind

The rapid expansion of the internet has provided tremendous opportunities to access unparalleled amount of data. An organization connects to the internet to gain access to information and to share information with the public, once a company connects its private network to the internet, that organizations private information becomes vulnerable to hackers, when private networks are connected to the internet, the risk are great. However, using some security measures, one can share public information and still protect

private information. One of these measures is to install a firewall between the private network and the internet (Blancharski 1998).

According to Tom Thomas "*A firewall is a security device that sits on the edge of your Internet connection and functions as an Internet Border Security Officer. It constantly looks at all the traffic entering and exiting your connection, waiting for traffic it can block or rejecting response to an established rule. The firewall is law and protection in a lawless global web. It is ever vigilant in its mission to protect the network resources connected to it*" (Thomas 2004).

The use of firewalls is no longer confined to servers, websites or commercial companies. Even if you simply dial in your ISP or use PPP (Point-to-Point protocol) to surf the internet, you simply cannot do without a firewall.

In a non-geek language; A firewall acts as a shield to protect your system from the untrusted, non-reliable systems connected to the Internet. Conceptually, it drives from the firewalls-barriers made of fire-resistant material-used in vehicles. A firewall on your PC however, listens to all ports on your system for any attempts defined set of rules. Putting it more technically; A firewall is a piece of software, hardware or both that allow only selected packets to pass from the internet to your private network or system.

2.4.2 Forms of firewall protection

Different types of firewall inspection protection exist, but in this paper we would only take 4 into consideration: (Panko 2003).

- Packet Inspection
- Application Inspection
- Network Address Translation (NAT)
- DoS Inspection.

Packet Inspection:

Packet Inspection focuses on the contents of IP, TCP, UDP and ICMP headers. Initially packet inspection employs static filtering, in which each packet is examined in isolation. However a number of attacks can be stopped only by stateful filtering, which accepts or rejects a packet primarily on the basis of whether it is part of an approved conversation or whether it is attempting to establish a legitimate conversation. Most firewalls now use stateful inspection.

Application Inspection:

Application inspection does not examine application message content. In contrast, application inspection uses programs called proxies to examine the contents of application messages contained in TCP and UDP data fields. Application inspection can stop many types of attacks that packet filtering cannot, such as malicious executable attachments.

Network Address Translation (NAT):

One danger is that an attacker will place a sniffer program outside the firewall and collect packet data. This will allow the attacker, among other things, to learn the IP addresses of internal hosts. NAT benignly spoofs the IP addresses of outgoing packets so that sniffers will learn only spoofed IP addresses and not the true IP addresses of internal hosts.

DoS Inspection:

Denial-of –Service inspection recognizes the inception of denial-of-service attacks and takes steps to alleviate them. Although the recognition of SYN flooding and few other common DoS attacks is widespread, denial-of-service inspection generally is fairly

rudimentary. The concept and details of DoS inspection is beyond the scope of this thesis, and would there for not be discussed.

2.4.3 Types of firewalls

Firewalls come in different types, each with its own strengths and weakness:

Screening Router Firewalls:

These are firewalls software that are already added or integrated into a router

Computer-Based Firewalls:

These are firewalls software added to Operating Systems, like Windows or Unix OS, example of these firewalls are Windows Defender, Antivirus Firewalls etc.

Firewall Appliances (Hardware-Based):

These are firewalls that come hardened in a box with no operating system other than the firewall on them, or come with a minimal OS.

Host Firewalls (Cloud-Based Firewalls):

These are firewalls that are installed on hosts themselves. These firewalls are installed just like an OS is installed. They are mostly installed on servers and sometimes on clients. They are normally used in conjunction with other firewalls.

For the purpose of this thesis we are going to look more into Hardware & Cloud-Based Firewalls:

2.4.4 Hardware vs. Cloud Based Firewalls

Hardware Firewalls:

Hardware Firewalls appliances are closed boxes that you simply plug into your router at one end and into your network at the other end. You power them up, turn them on, and use them immediately. Firewall appliances either have no operating systems or minimal operating systems. This makes them fast for a given performance requirement level.

Firewall appliances come pre-packaged with a good set of filtering rules, making them suitable for smaller firms that lack the security staff needed to optimize filtering rules. Of course, as threats grow, rules need to be updated. Most firewall vendors provide rule updates, much as antivirus vendors provide virus signature updates for their software.

Cloud-Based Firewalls (Host Firewalls):

One approach is to add firewall software to individual client and server hosts. In contrast to other firewalls, these host firewalls protect only the hosts on which they operate. Cloud firewalls can be configured with knowledge of the specific host. For instance, if the host is a webserver, only web service requests should be allowed through.

2.4.5 Firewall Pros & Cons

	Advantage	Disadvantage
Hardware	• No OS, makes it difficult to hack • Minimal Setup	• No or minimal updates • Not customized
Cloud	• Host knowledge	• Hard Configuration

	• In-depth defense	• Configured by ordinary users

Table 1: Hardware vs. Cloud-Based Firewalls (Panko 2003).

2.4.6 Access Control List

All information that flows across the Internet uses TCP/IP. And in turn, this information is sent in small pieces known as packets. In the early days of the internet, filtering based on packets was common and in many cases, routers in many networks still use packet filtering. The methods used to configure and deploy packet filters on Cisco ASA and router's is known as access control list (ACL). There are two main types of ACL's: the standard ACL, which filters based on IP address, and extended ACLs; which look further into packet header, if so configured (Thomas 2004).

An access list is essentially a list of conditions that categorize packets. They can be really helpful when you need to exercise control over network traffic. An access list would be your tool of choice for decision making in these situations.

One of the most common and easy to understand uses of access list is filtering unwanted packets when implementing security policies.

Types of ACL's

There are two main types of access-list: (Lammle 2011).

1. Standard Access Lists: This uses only the source IP address in an IP packet as the condition test. All decisions are based on the source IP address. This means that standard access lists basically permit or deny an entire suite of protocols. They don't distinguish between any of the many types of IP traffic such as Web, Telnet, and UDP and so on.

2. Extended Access Lists: Extended access list can evaluate many of the other fields in the layer 3 and layer 4 headers of an IP packet. They can evaluate source and destination IP addresses, the protocol field in the Network layer header, and the port number at the Transport layer header. This gives extended access lists the ability to make much more granular decisions when controlling traffic.

More in-depth about standard and extended access list can be found on Cisco books which are beyond the scope of this thesis.

CHAPTER THREE
LITERATURE REVIEW

3.1 Literature Review Process

In this thesis, we look into different ideas from different participants of cloud security, network security, and information security. There was no particular research related to the new architecture we did, but relevant test and researches which lead to the conclusions on different firewall the architecture should be had been done. We conducted a literature review of what had been published based on ideas and there are many articles, book and publications on information security, cloud computing and firewalls. Most of these materials are written to explain and propose a method of implementing information security, difference in forms of security and policies. Knowledge about previous research related to this type of architecture is very crucial. In this section we reviewed previous research work. The search for scholarly articles, journals, and conference paper were extracted from Google Scholar, IEEE Xplore digital library, ACM digital library database and Georgia Southern University digital commons. Terms like Firewalls performance, packet filters, cloud firewalls, hardware firewalls, network security, Vyatta, virtualization, and Cisco ASA were used to filter the search.

The table below shows the result of number of articles found after using the search filters.

	Firewall Performance	Packet Filters	Cloud Firewalls	Hardware Firewalls	Network Security	Vyatta	Virtual ization	Cisco ASA
Google Scholar	X	X	X	X	X	X	X	X
IEEE Xplore	447	3780	61	205	53,980	1	4,066	2
ACM	10,635	14,575	1437	6341	125,405	36	10,627	210
Digital Commons	4	3	1	1	84	0	7	0

Table 2: Literature Review Search Filters

3.2 Related work

Certain numbers of works have been made in related to above mentioned criteria in information security; cloud computing, computer network security and virtualization. The areas covered in this review includes: Cloud Security, Network Security, and Cloud Computing & Virtualization.

3.2.1 Firewall Performance

Firewall performance is one of the top research topics in information technology, be it that of hardware or cloud based firewalls. Some researchers focus on evaluating performance of firewalls in Gigabit-Networks (Funke et. al 2002). The authors present the result of a measurement study of packet screen performance. A cluster computer was used to generate internet traffic that is large enough to saturate a Gigabit connection using NetPerf from HP as the measurement tool. The result of this research shows that packet

filtering can be performed almost at wire speed even for gigabit links. (Lyu & Lau 2000) explores the firewall security and performance relationship for distributed systems. The security test experiments are performed in a LAN in which a firewall is set up as the entry point for all traffic going in and out of the LAN. Two test are conducted in the research, one of which is the security testing, in which security checkups and penetration testing are applied in testing the security of the firewall, the second being a performance test, which is done on the firewall to measure the relative performance degradation of two types of service, i.e. HTTP and FTP of the firewall. The result of the security after analysis was proved based on certain policies set during the test, and that of the performance test. The total transaction time and latency are found in different test scenarios under the firewall security policies created. (Sossa et. al 2012) compares the performance of a software-based router and that of a hardware-based router using a practical approach. The test uses Vyatta running as the virtual software router (VSR) and Cisco ASA as the hardware router. Before the test was carried, a comparative feature of both devices was analyzed. The performance measurement focused on convergence time, delay and throughput. The result of the general performance showed high stability in standard deviation for Vyatta routing solutions, with a predictable behavior for convergence time, delay and throughput design parameters. The convergence time in Vyatta is low. The test result shows the software speed. Conversion time over Vyatta in comparison with Cisco ASA is 70% better while Cisco ASA has a better throughput. (Su & Xu 2013) did a master's thesis which evaluates the performance of Cisco ASA and Linux Iptables Firewall; the main parameters for this test were Throughput, Latency, and Concurrent Sessions using different performance monitoring tools. These three parameters test were implemented and the results shows

that the throughput values for both firewalls belong to the same level, with that of the Cisco ASA 5505 a little bit higher than Linux iptables, even though the hardware resources of Cisco ASA 5505 are worse than that of the Linux iptables. The latency result shows no big difference between the two firewalls. But the Cisco ASA 5505 delay is slightly lower than Linux iptables. Also the result of the concurrent session shows that below 8,000 connections the performance of Cisco ASA 5505 and iptables are almost the same, between 8000 and 10,000 connections there is a seldom failure. However after 10,000 requests, large number of failure gradually appears on Cisco ASA 5505. It reaches to the highest value of 162.5 corresponding to 15,000 requesting clients. However, Linux iptables firewall always keeps a relative low level although with maximum request.

(Sheth & Thakker 2013) evaluates and compares the performance of network firewalls under DDoS attack; the authors performed the comparison using an open packet filter (PF) firewall, Checkpoint SPLAT and Cisco ASA 5505 in a testing environment with laboratory generated DDoS performance parameters. JMeter was used as the load testing tool, and various parameters were used in making decision, such as HTTP throughput, Legitimate Traffic allowed till percentage of DDoS traffic, Firewall CPU Utilization of DDoS, Time for complete failure (unreachable) at full DDoS, Capacity limits (% of other traffic blocked except TCP). The performance testing results indicated that no firewall proved to be capable of withstanding DDoS for longer time. Checkpoint showed initial resistance and allowance of legitimate traffic at percentage more than Cisco ASA and PF. However CPU utilization of Checkpoint was higher as compared with Cisco ASA and PF firewalls.

(Sheth & Thakker 2011) performed a performance evaluation and comparative analysis of network firewalls. In conjunction with the research in (Sheth & Thakker 2013),

this time around the author focused on detailed analysis and comparison in terms of costs, security, operational ease and implementation of Open source packet filter (PF) firewall using Checkpoint SPLAT and Cisco ASA in a testing environment with laboratory generated traffic. Various throughputs and connections statistics were used as benchmark for performance comparison. The results indicated that Cisco ASA outperforms its peers in most performance criterions. Checkpoint SPLAT and OpenBSD PF also provides reasonably good and competitive performance. The result can be useful in comparing vendors to procure firewall based on one's own organizational requirements. (Acharya et. al 2006) conducted a traffic-aware firewall optimization strategy. In the paper they developed a novel adaptation mechanism that dynamically detects anomalous traffic behavior and adaptively alters the firewall rules to avoid serious performance degradation due to the traffic anomaly. To evaluate the performance they collected a large set of firewall rules and traffic logs at tens of enterprise networks managed by a Tier-1 service provider. Their evaluation results find these approaches very effective. They actually achieve more than 10 fold performance improvement by using the proposed traffic-aware firewall optimization.

3.2.2 Cloud & Virtualization Security

Considerable amount of research have been made based on Cloud & Virtualization Security (Basak et al 2010) explained virtualization, networking and security in the cloud. The paper highlights a new trend in the industry used to virtualize network security (netsec) functions inside security virtual appliances (SVAs), which can then be placed on hosts, and offers a distributed security functions for network flows across the cluster. They analyzed the trend in details using VMware vShield product line as an example. The approach replaces single choke-point based physical security devices like firewalls, IP

address management (IPAM), flow monitoring, and data leakage prevention (DLP) with distributed virtual counterparts running on slices of x86 co-located with compute workloads with ability to tap into traffic going in and out of virtual machines (VMs). They highlighted some important benefits of virtualized netsec that was not possible in the physical world. They established that a virtualized netsec deployment like vShield firewall effectively creates a firewall enforcement presence in front of every vNIC. Every network packet that do not need to leave the host are seen by the vShield firewall. Thus the vShield firewall does not suffer from blind spots that a physical firewall cannot address. The vNIC level firewall allows achieving additional security policies with ease and creating a secure Ethernet transport environment.

(Subashini & Kavitha 2010) conduct a survey on security issues in IaaS, PaaS and SaaS service delivery models of cloud computing. The research identified some key elements of each service delivery models, with that of SaaS application development and deployment process as: Data Security, Network Security, Data Locality, Data Integrity, Data Segregation, Data Access, Authentication & Authorization, Data Confidentiality, Web Application Security, Data Breaches, Virtualization Vulnerability, Availability, Backup and Identity Management & Sign-on process. Each of the security issues of the SaaS model are discussed clearly in the paper. The article states that "In PaaS, the provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider and provider has to offer strong assurances that the data remains inaccessible between applications, PaaS is intended to enable developers build their own applications on top of the platform. Which as a result tends to be more extensible than

SaaS, at the expense of customer-ready features? This tradeoff extends to security features and capabilities, where the built-in capabilities are less complete, but there is more flexibility to layer on additional security". The paper also mentioned the security issue in IaaS as prone to various degrees of security issues based on the cloud deployment model through which it is being delivered.

(Adams & Agesen 2006) did a comparison between Software and Hardware techniques for x86 virtualization. They compared existing software VMM with a new VMM designed for the emerging hardware support. The hardware VMM often suffers lower performance than the pure software VMM. They studied architecture level events such as page table updates, context switches and I/O, and find their costs vastly different among native software VMM and hardware VMM execution. During the experiment, they examined a number of 64-bit workloads under VMware Player 1.0.1's software and hardware assisted VMMs. The study shows that software VMM outperforms the hardware VMM. The compute intensive benchmarks run essentially at native speed on both VMMs. However, as workloads include progressively more privilege operations (context switches, memory mapping, I/O, interrupts, system calls), both VMMs suffers overheads. Using a series of increasingly targeted benchmarks, they showed how and why the software VMM usually outperforms the hardware VMM.

CHAPTER 4
METHODOLOGY

4.1 Methodology

This work focused on carrying out different types of test to obtain the results for the research objectives stated earlier. Furthermore, we implemented a secured network architecture with 2 firewalls of different platforms. One using a cloud-based and the other using a hardware-based. Both firewalls are designed to work together in other to provide a great secured architecture and optimize performance. To achieve this; different types of test were set in place. The tests were categorized in two phases. Phase one is the pilot test which has 4 different test. These tests are: Control test, Cloud test, Hardware test, and a federated test. (All 4 test of phase one would be discussed later in this chapter). Two scenarios, performance load test and a spike test were used to evaluate the performance of each model, how each model handle packets (using 10,000 packets) was carefully analyzed. Throughput of both performance and spike test of each model was compared. The second phase of the test which is the simulation test is designed to stress the firewalls in other to identify weaknesses. It has 2 different tests, one of which is a federated test and the other is a cloud-based vs. hardware test. These phase two tests use more traffic and resources. Lastly an approach on how to forward packets under certain heuristics from hardware-based firewall to the cloud-based firewall in a federated architecture was proposed. These heuristics rules will define the conditions and criteria in which services would be transferred to the cloud firewall to achieve optimum performance and outcome, when the hardware firewall becomes stressed.

4.2 Required Resources

To carry out these tests, different resources would be needed, all of which would be discussed below:

4.2.1 Cisco ASA 5510

The ASA (Adaptive Security Appliance) 5510 version 8.3 series is a hardware-based firewall that gives solutions that are specifically designed to the highest safety and excellent VPN services, with innovative scalable service architecture. It is the core component of the Cisco Self Defending Network. The Cisco ASA 5510 series can provide proactive threat defense, network activity control and application traffic control. It also delivers flexible VPN connection. The lower models are not only for protection of the home, office or branch office but can also protect the small and medium-sized enterprises. The higher models can protect the large enterprises networks and give them in-depth security protection. It can reduce the overall deployment costs and operating complexity. The Cisco ASA 5510 Adaptive Security Appliance is a next generation, full-featured security equipment. It is suitable for small businesses, branch offices and medium sized enterprises. It provides IPSec, SSL VPN and rich networking services (Su & Xu 2013).

4.2.2 Vyatta VC6.6

Vyatta VC6.6 is a cloud-based virtual firewall for IP networks. Vyatta system firewall functionality provides the following (Vyatta 2012).

- Packet Filtering for traffic. Traversing the router using in and out keywords on an interface.
- Packet filtering for traffic; destined for the router itself, using the local keyword.

- Definable criteria for packet-matching rules, including source IP address, destination IP address, source port, destination port, IP protocol, and ICMP type.
- General detection on IP options such as source routing and broadcast packets.
- Ability to set firewall globally for stateful and stateless operation.

The Vyatta firewall features both IPv4 and IPv6 stateful packet inspection to intercept and inspect network activity and allow or deny the attempt. Vyatta's advanced firewall capabilities include stateful failover, zone-based firewalling, time-based firewalling and more. Vyatta is used as the cloud-based firewall in this thesis.

4.2.3 Cisco Network Switch

A switch is a network device that serves as a controller, enabling network devices to talk to each other efficiently. It processes and forwards data at the data link layer (Cisco 2014). A switch is used to connect the different devices used in this thesis.

4.2.4 Windows 7 Operating System

Windows 7 is an operating system designed by Microsoft for use on computers. Windows 7 comes in 32 bit and 64 bit versions. Four Windows 7 Virtual Machines with master/slave JMeter remote/distribution test setup are installed on a VMware ESXi hypervisor.

4.2.5 JMeter

JMeter, an Apache desktop application is an open source software, designed to test load functional behavior and measure performance (Apache 2013), with a focus on web applications. JMeter is not very scalable and a maximum of 2500 requests per second can be sent using single system in a setup (Apache, 2013). This limitation results in JMeter

client machine not to stimulate (performance wise) enough users to stress the server. To improve performance and generate more traffic, JMeter can be run remotely from a single JMeter GUI client. By running JMeter remotely, it can replicate a test across many low-end computers and thus stimulate larger load traffic (Apache, 2013).

JMeter is used remotely with one master and three different slaves to generate enough traffic spikes to max out the targeted server.

JMeter is installed on four Windows 7 virtual machines with one being the master running the JMeter GUI and controlling each slave, and 3 of the virtual machines as slaves running JMeter-server, which receives command from the master and to send traffic to the server under test. A basic remote-test using server-slave layout is shown below:

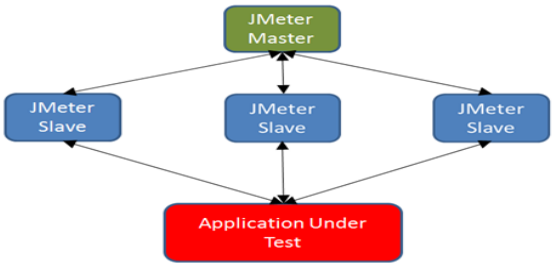


Figure 11: JMeter Master/Slave

4.2.6 ESXi Hypervisor

Two servers each with an ESXi hypervisors are used in this research. One of the hypervisors has an Ubuntu web server running as a VM with Vyatta as the cloud-based firewall, and the other server has an ESXi hypervisor with 4 windows 7 VM's running.

4.2.7 Ubuntu Cloud Webserver

A cloud webserver is configured as the target on a Ubuntu Linux Distribution, The Ubuntu Linux is installed as a VM on one of the servers.

4.2.8 62 Standalone Computers

62 Standalone Computers with windows 7 operating system are used for the second phase of this work. One of the computers has vSphere Client installed on it, three of the computers have JMeter masters installed, and the remaining 58 computers have JMeter slaves installed. vSphere Client is the management software used to control the VMware ESXi hypervisor.

4.3 Phase I: Pilot Test

A pilot test was conducted using less traffic aimed to compare and evaluate performance of the different models. Under the pilot test four different types of test are carried out, all of which are discussed below; this test uses the four windows 7 VM's with one JMeter master and 3 JMeter slaves.

4.3.1 Control Model

This test is carried out with no software or hardware firewall, the figure below shows the architecture of the control test:

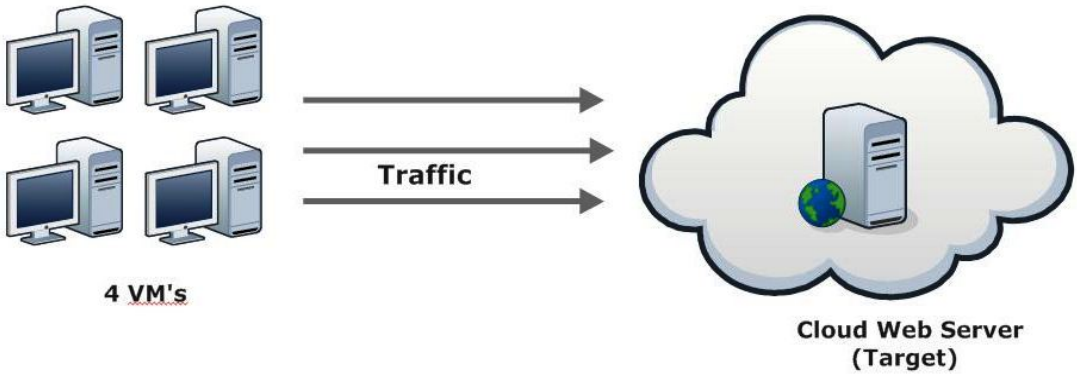


Figure 12: Control Model

4.3.2 Hardware Model

The hardware test is carried out using only the Cisco ASA firewall as the filter. The figure below shows the hardware-based filtering architecture:

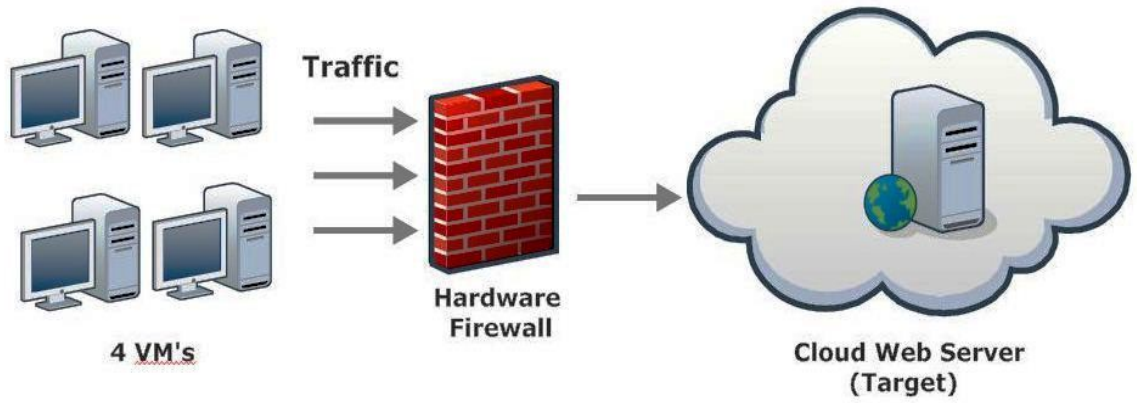


Figure 13: Hardware Model

4.3.3 Cloud-Based Model

The cloud-based test is carried out using only Vyatta as the firewall filter. The figure below shows the cloud-based filtering architecture:

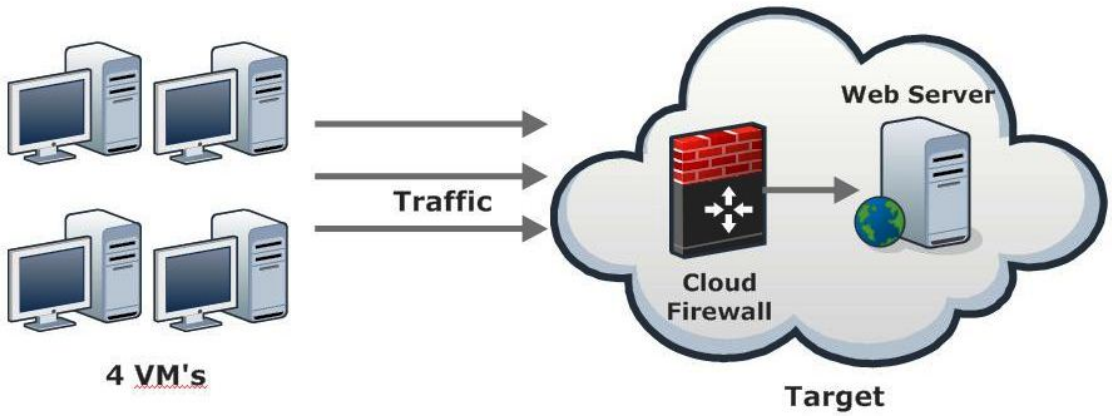


Figure 14: Cloud Model

4.3.4 Federated-Model

This is a hybrid model; this test was carried out using firewalls, Cisco ASA and Vyatta, the hardware-based and the cloud-based. The figure below shows the architecture of how the test was carried out.

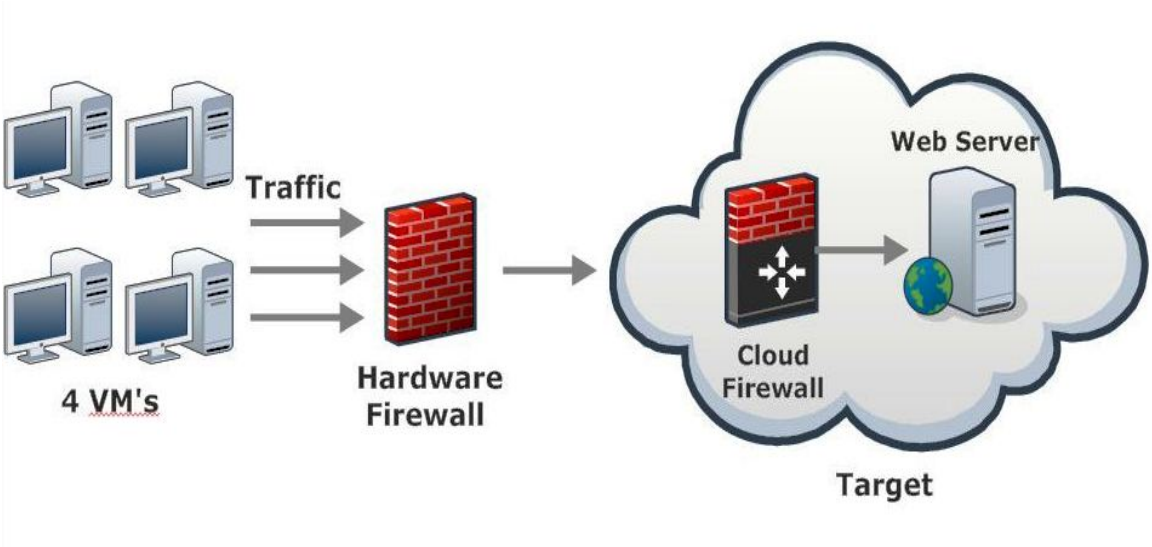


Figure 15: Federated Model

4.4 Phase II Simulation Test

Phase II test uses more traffic, it used 61 standalone computers, with 3 JMeter masters and 58 slaves. It is aimed at stressing the firewalls to see which firewall can handle more traffic. Two tests were carried out under this test all of which are discussed below:

4.4.1 Test I - Federated Model

This model uses both firewalls and the figure below shows the architecture of the model. It is designed to stress both devices and max them out.

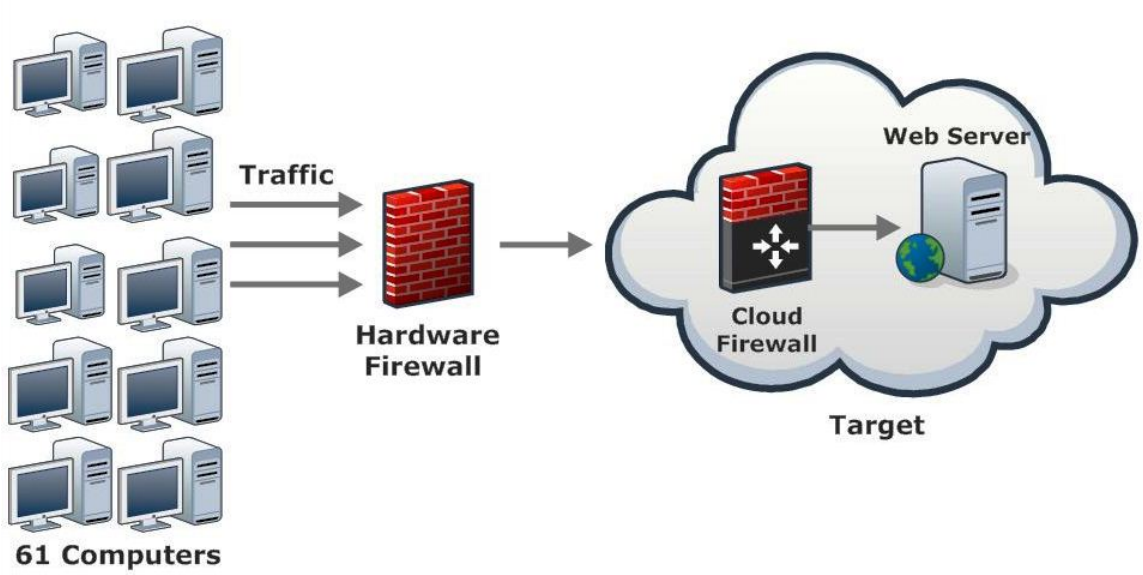


Figure 16: Phase II Federated Model

4.4.2: Test II – Hardware vs. Cloud-Based Models

These two tests compare the performance of both devices under a heavy bearable traffic. The figure below shows the architecture of the models.

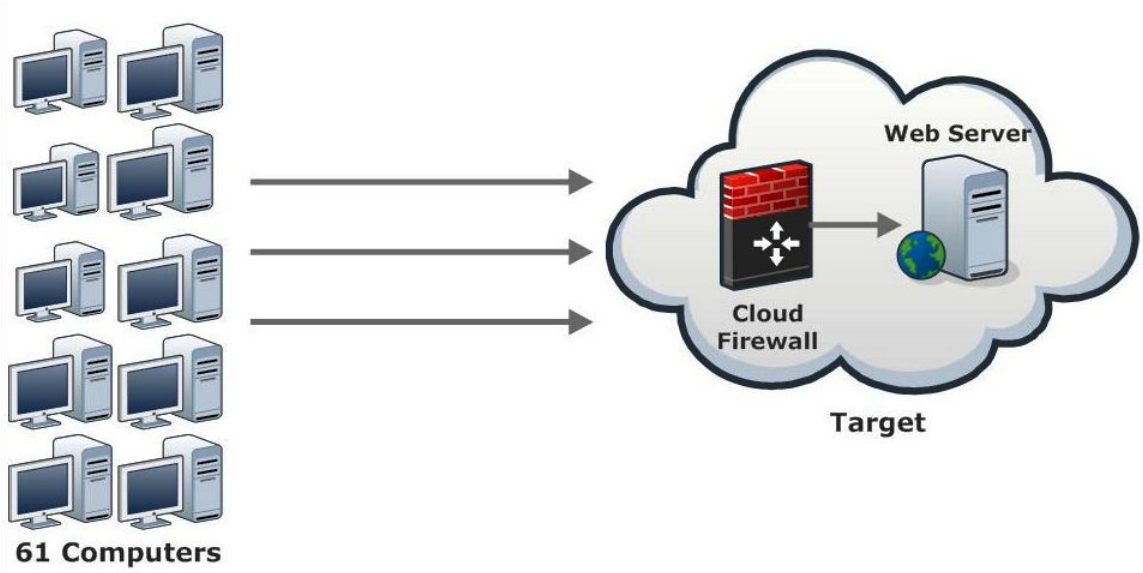


Figure 17: Phase II – Cloud Model

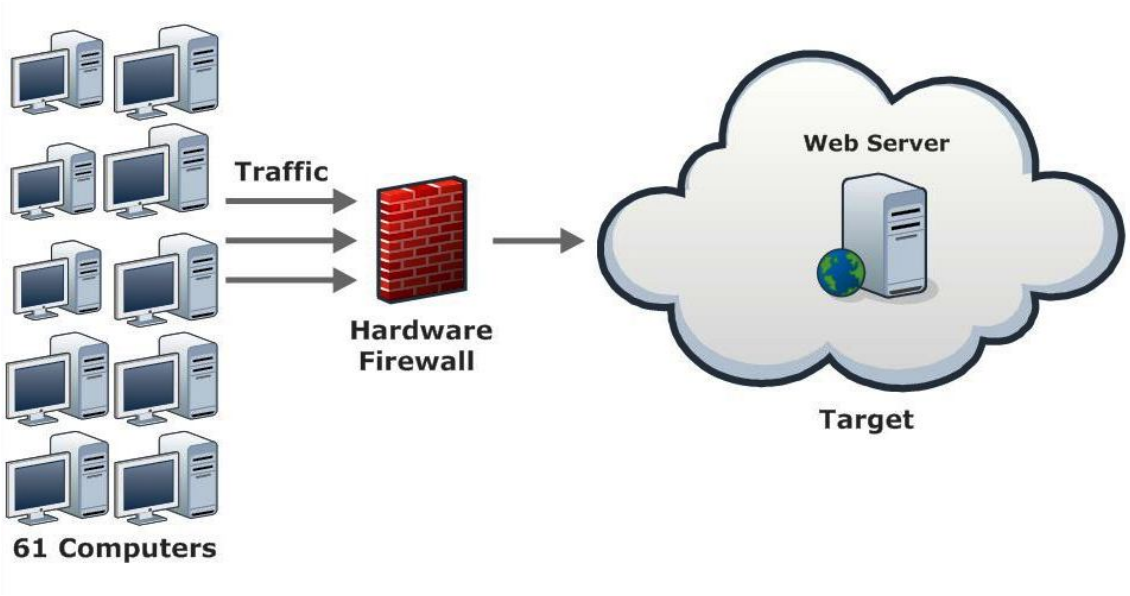


Figure 18: Phase II – Hardware Model

4.5 Metric Factors & Thresholds

Some factors and conditions need to be met in other for migration to occur from the hardware to the cloud-based. These factors are what render the hardware firewall incapable of filtering packets, or result in lower performance.

In this research these metric factors are:

- Memory – Memory Utilization
- Processor – CPU Utilization
- Packet Drops

4.5.1 Metric Factors

Memory:

This is the allocated flash memory of the device. For better performance, memory utilization should always be at a lower level, but some condition can result to high memory utilization.

Processor:

When CPU utilization is high, it affects the performance of the Cisco ASA. Several factors usually results to high CPU utilization, some of which are concurrent connections, traffic load etc.

Packet Drops:

This is the discarding of legitimate packets when a device is overloaded or stressed and cannot perform the required packet filtering. In this thesis, we sent legitimate packets to the devices; therefore a higher number in packet drops means that the device is not performing as required.

4.5.2 Thresholds

Device Thresholds

The maximum defaults for the Cisco ASA device are:

Max Thresholds:

Packet drop => 5%

Memory Utilization => 85%

CPU Utilization => 75%

Component	**Metrics**		**Threshold**
Memory	DRAM	Pre Cisco ASA 8.3 OS	256MB
		Post Cisco ASA 8.3 OS	1GB
		Default	1GB
	Compact/System Flash	Minimum	256MB
	Memory Utilized		

Processor	CPU Utilized*	Default High Threshold	Over 70%
		Critical High Threshold	Over 95%

Table 3: Cisco ASA Threshold

4.6 Result Parameters.

Two scenarios are used to collect and analyze the results of the pilot and simulation test. These are:

a. Traffic Spike test

b. Endurance test

The results of both the spike and endurance test are compared for each model in the different phases. Also throughput and mathematical calculations using statistics are compared.

4.6.1 Spike test

Spike testing is a load test in which a device undergoes a performance test in order to verify the device stability during a burst of concurrent user or system activity to varying degrees of load over varying time periods. JMeter is configured to send traffic to be used for spike testing.

4.6.2 Endurance Test

Endurance Test is a test carried out to verify if a device or system can withstand the processing load it is expected to have endured for a long period of time. In this test, memory consumption is usually observed to determine potential failures.

4.6.3 Throughput

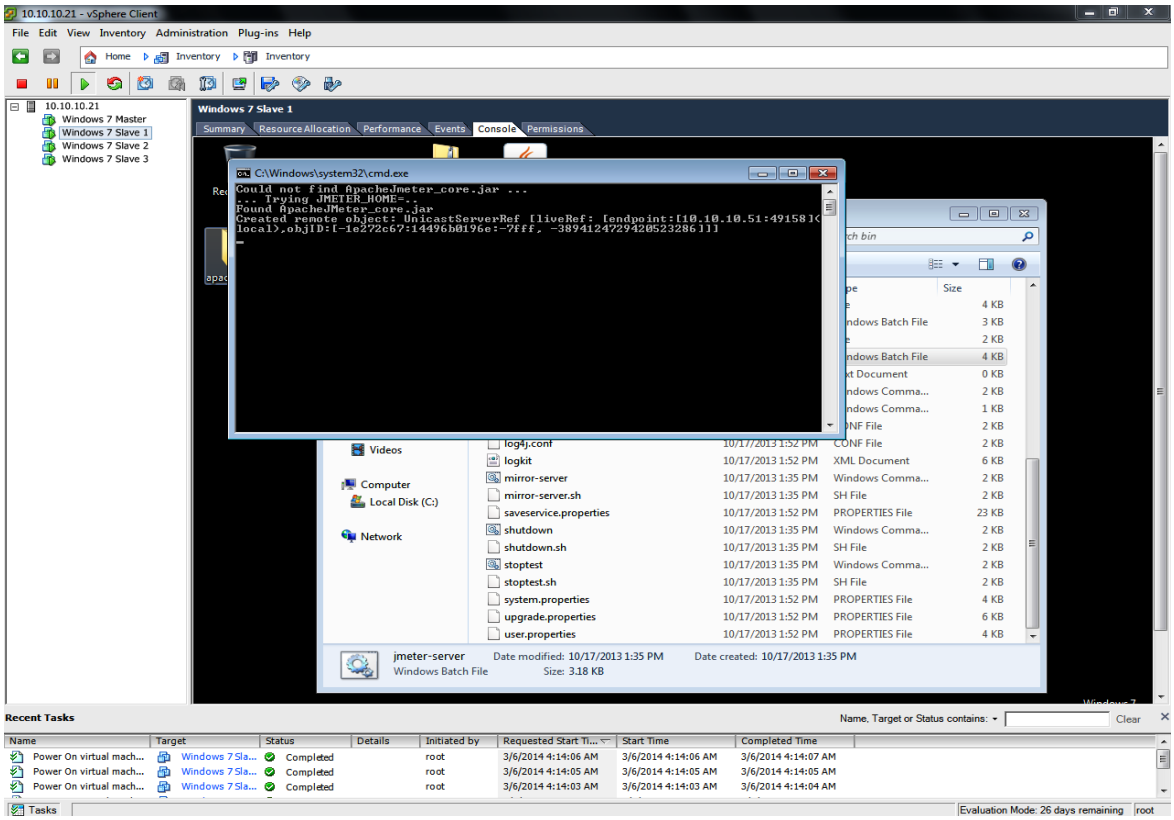
Throughput is the amount of work a device can do in a given period of time. In this thesis we calculate throughput based on how many packets are transmitted per second.

CHAPTER FIVE
IMPLEMENTATION

5.1 Devices Implementation

5.1.1 Windows 7 Virtual Machines setup

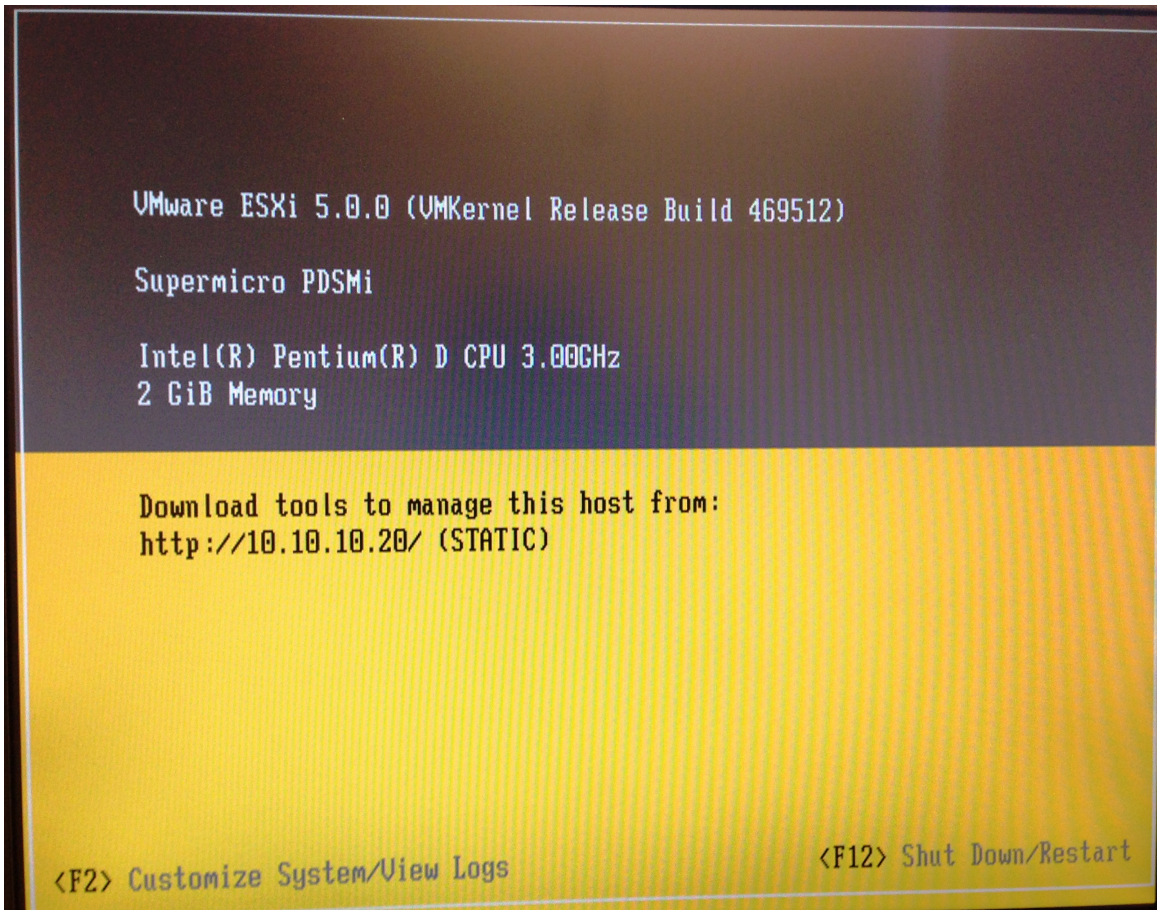
In this thesis 4 windows 7 virtual machines are used, and they are all hosted on an ESXi hypervisor running on a Supermicro server. The windows 7 are connected using a vSwitch. Each of the four 64-bit Windows 7 VM's has an Intel(R) Xeon (R) CPU E3-1245 V2 running at 3.40GHz processor speed, with 1GB of RAM and 60GB HDD. The screen shot below shows the Windows 7 VM's running on an ESXi hypervisor.



Screen shot 1: Windows 7 VM's screenshot

5.1.2 ESXi Hypervisor

Two VMware ESXi 5.0 hypervisor running on Supermicro servers are used. The minimum requirements for ESXi hypervisors are: Two processors running at 2GHz speed, 6GB RAM, 2x1GB network adapter and 100GB storage. The screen shot below shows the ESXi hypervisor running on one of the servers.



Screen Shot 2: ESXi screenshot

5.1.3 Servers

Two servers are used in this thesis, one of which is a Supermicro X9SCL/X9SCM, with Intel(R) Xeon (R) CPU E#-1245 V2 @ 3.40GHz with 32GB of RAM and 1TB of storage. This server has the ESXi hypervisor with the four windows 7 VM's and the other server is a

Supermicro PDSMi server with Intel(R) Pentium (R) D CPU @ 3.00GHz and 2GB of RAM with 750GB of storage. This server has the ESXi hypervisor with the Linux Ubuntu Web Server VM and Vyatta Cloud-Based firewall.

5.1.4 Switches

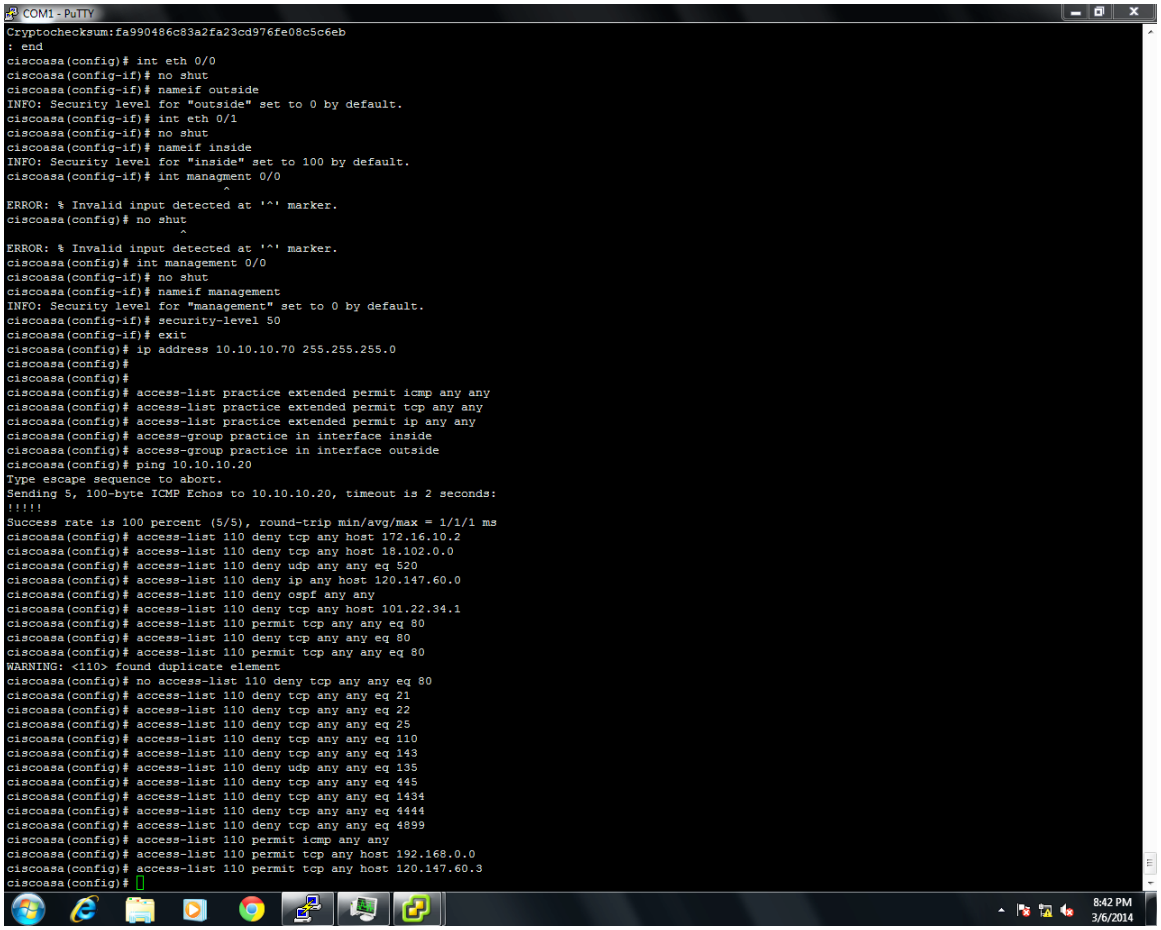
Two Cisco Switches are used. One of the switches is used for the internal network and the other is used for the outside network. The switches are Cisco smart switches which means that no configuration is needed for the switch.

5.1.5 Virtual Switch (vSwitch)

3 vSwitches are used. One of the vSwitch connects the four Windows 7 VM's, another connects Vyatta with the webserver as the inside network and the last connects Vyatta with the outside network.

5.1.6 Cisco Adaptive Security Appliance (ASA)

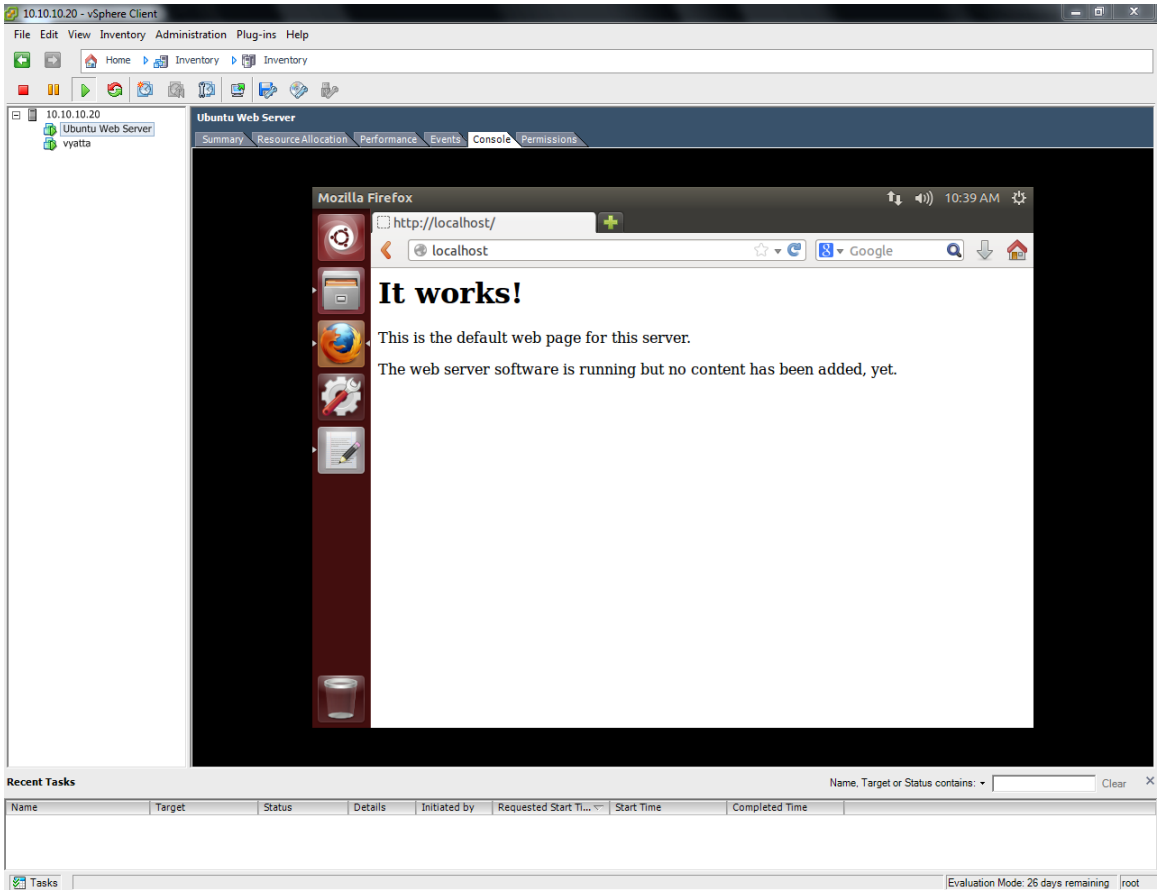
One Cisco ASA firewall is used. The Cisco ASA is version 8.3 with 2GB of RAM. The Cisco ASA is configured to allow and block specific packet. The basic commands used to configure the Cisco ASA and the firewall rules used are listed in the Appendix B&C. The screen shot below shows both the command and firewall rules on the Cisco ASA. Different rules are applied to both inbound and outbound traffic of both inside and outside interfaces.



Screen Shot 3: Cisco ASA commands and firewall rules.

5.1.7 Ubuntu Cloud Web Server

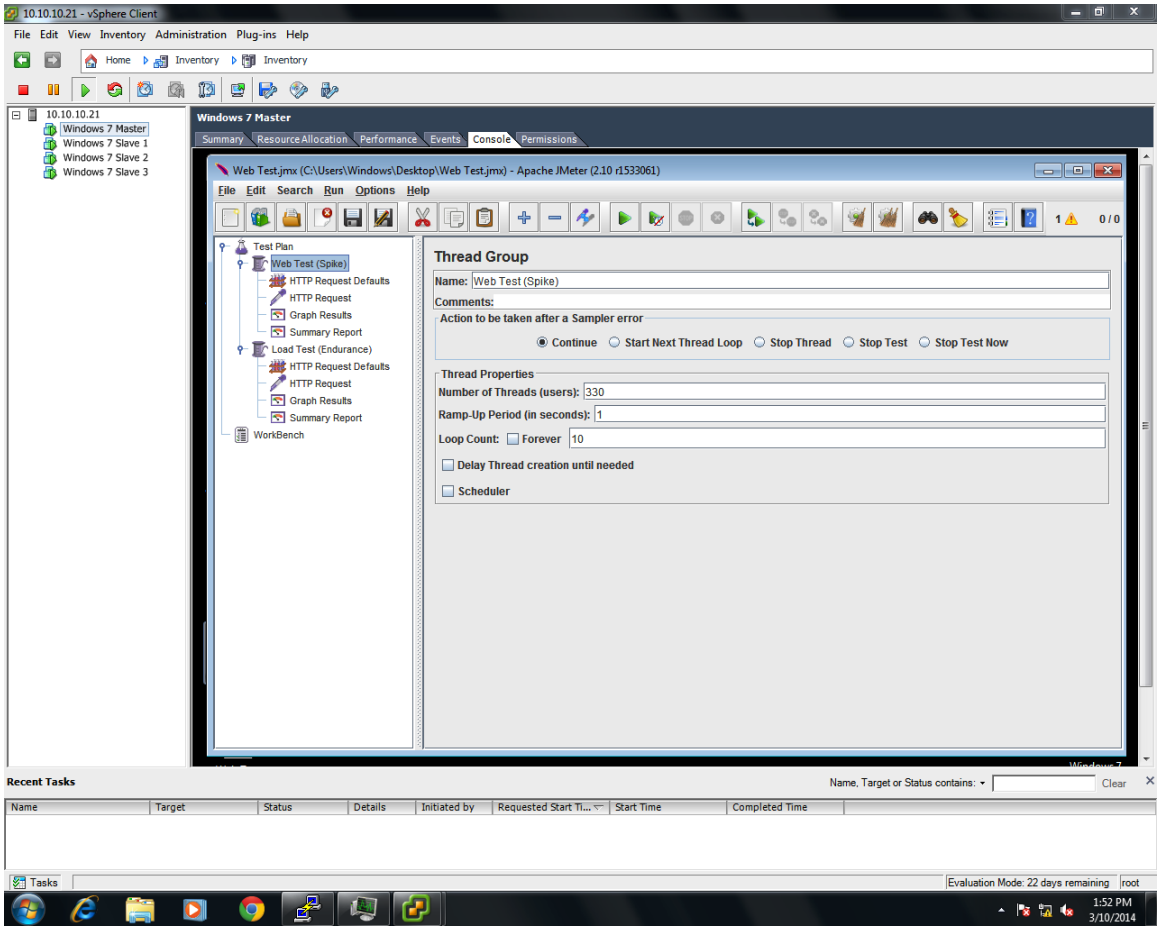
A cloud web server is installed inside Linux Ubuntu 13.04 Distribution VM. The 64bit Linux Ubuntu is installed as a VM on one of the servers with the ESXi hypervisor. The Ubuntu VM has an Intel(R) Pentium ® D CPU @ 3.00GHz processor, 1GB of RAM and 50GB of storage. A screen below shows the webserver running on Ubuntu 13.04.



Screen Shot 4: Ubuntu Web Server

5.1.8 JMeter

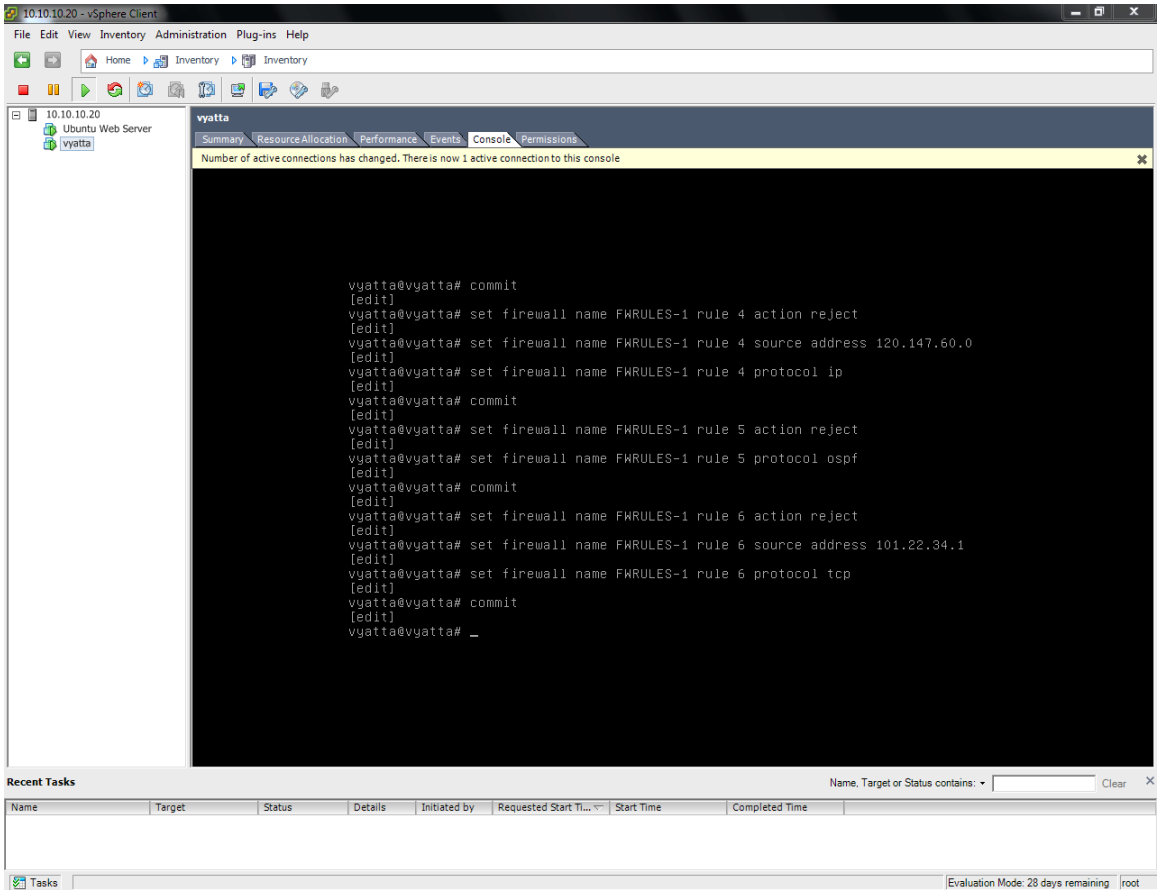
Four JMeter's configured as a master/slave are installed on the Four Windows 7 VM's. JMeter is a 100% Java application, and therefore requires a fully compliant JVM. JMeter is configured in 2 forms for two different types of scenarios which are spike and endurance. All scenarios are designed to send legitimate HTTP packets to the webserver. A screen shot showing both configurations is shown below:



Screen Shot 5: JMeter.

5.1.9 Vyatta Cloud Firewall

Vyatta Cloud Firewall runs on one of the ESXi hypervisor as a VM. The Vyatta has 512MB of RAM, 2 Network Adapters for the inside and outside network, and 8GB of storage. The Vyatta firewall uses some basic commands to configure and define firewall rules (see appendix A). A screen shot showing Vyatta commands and firewalls is shown below:



Screen Shot 6: Vyatta command and firewall rules.

5.1.10 Standalone Computers

62 Standalone computers are used: One of the computers has vSphere client installed on it, which is used to monitor the 2 ESXi hypervisors. Three of the computers have JMeter masters installed. Two of the JMeter masters are used to generate traffic, and the last JMeter master is used to monitor the traffic. Lastly, the remaining 58 computers have JMeter slaves installed. They receive instruction to send traffic from the 2 JMeter masters.

5.2 Models Architecture Configurations & Implementation

5.3 Phase I: Pilot Test

Implemented to test and evaluate performance under normal traffic.

5.3.1 Control model

The control model which uses no firewall used the four windows 7 VM's with JMeter installed. Two vSwitches one connecting the Windows 7 VM's and the other connecting the webserver with the rest of the network are used, 2 ESXi hypervisors, for Windows 7 VM's and Ubuntu Cloud Web Server, 2 servers for the ESXi hypervisors, 1 Standalone Computer with vSphere installed for ESXi hypervisor maintenance and one Cisco Smart Switch to join the two separate network. An in-depth architecture of the control model is shown below with IP address and subnets shown in Appendix D.

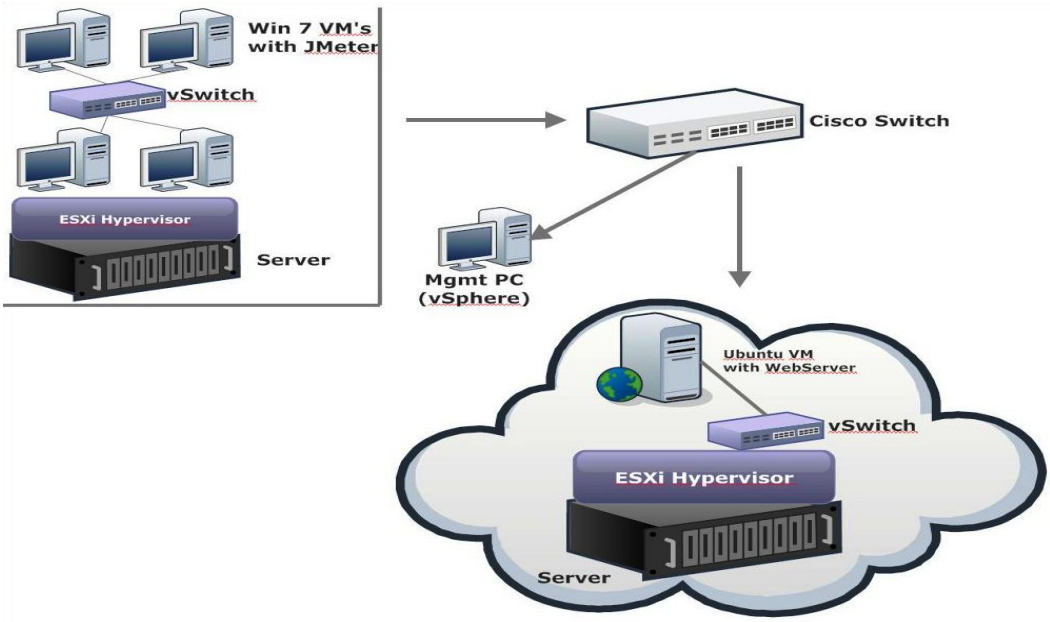


Figure 19: Control Architecture

5.3.2 Cloud-Based Model

The cloud-based model which uses only one firewall, (Vyatta firewall) used four windows 7 VM's with JMeter installed, three vSwitch, one connecting the four windows 7 VM's, another connecting Vyatta with the outside network, and the other connecting Vyatta with the inside network (Webserver), Vyatta cloud-based firewall, Ubuntu webserver, 1 Cisco Smart Switch to join the two separate networks, 2 servers for the ESXi hypervisors, and one standalone computer with vSphere client installed for ESXi hypervisor maintenance were used. The cloud-based architecture is shown below with its IP addresses and subnets configuration shown in Appendix D.

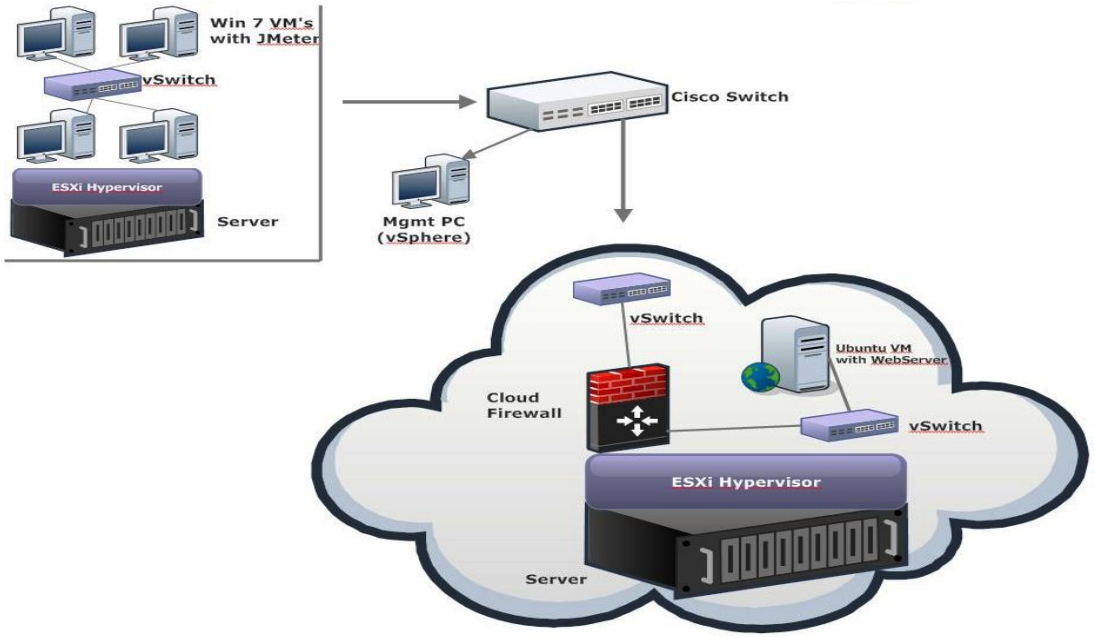


Figure 20: Cloud-Based Architecture

5.3.3 Hardware Model

The hardware model used only one firewall (Cisco ASA), four windows 7 VM's with JMeter installed, two vSwitch one for the windows 7 VM's and the other for the Ubuntu

cloud webserver, 2 ESXi hypervisors, 2 Servers, Ubuntu cloud webserver, one Cisco ASA firewall, two Cisco Switches, and one standalone computer with vSphere Client installed. The hardware model architecture is shown below with its IP addresses and subnets configuration shown in Appendix D.

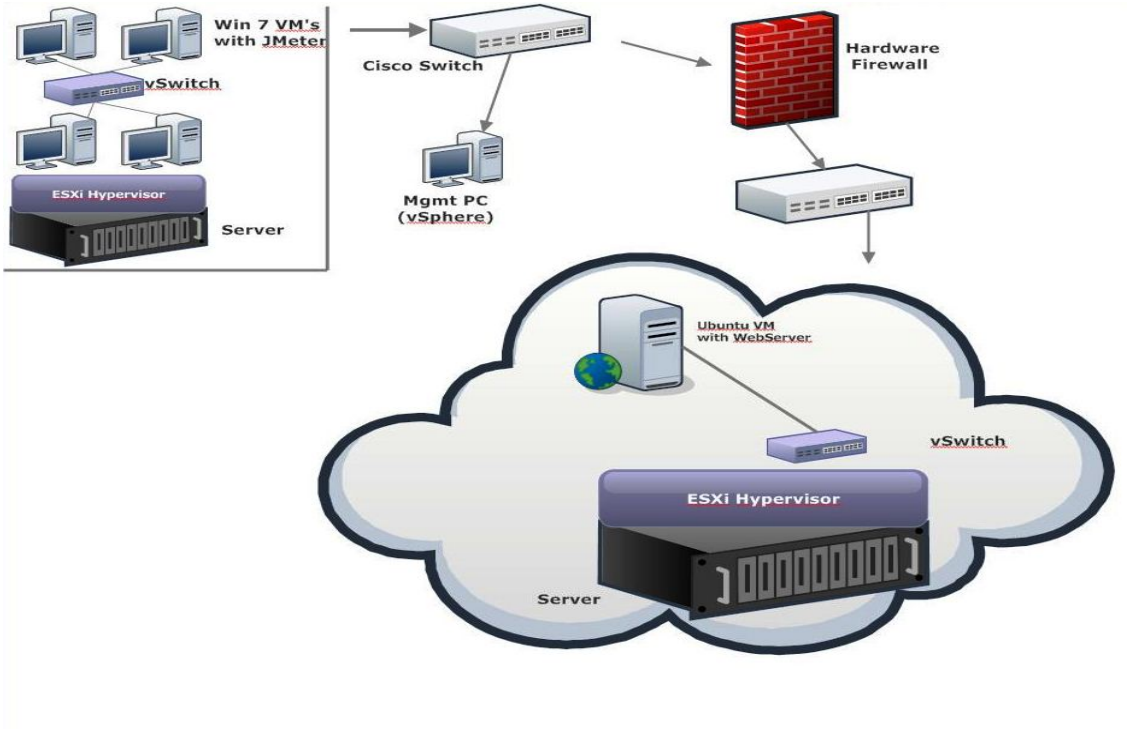


Figure 21: Hardware Architecture

5.3.4 Federated Model

The federated model used two firewalls (Vyatta & Cisco ASA). It also used four windows 7 VM's with JMeter installed, three vSwitch one for the windows 7 VM's another for the Ubuntu cloud webserver & Vyatta and the other for Vyatta and the outside network, 2 ESXi hypervisors, 2 Servers, Ubuntu webserver, two Cisco Switches, and one standalone computer with vSphere Client were also used. The federated model architecture is shown below with its IP addresses and subnets configuration shown in Appendix D.

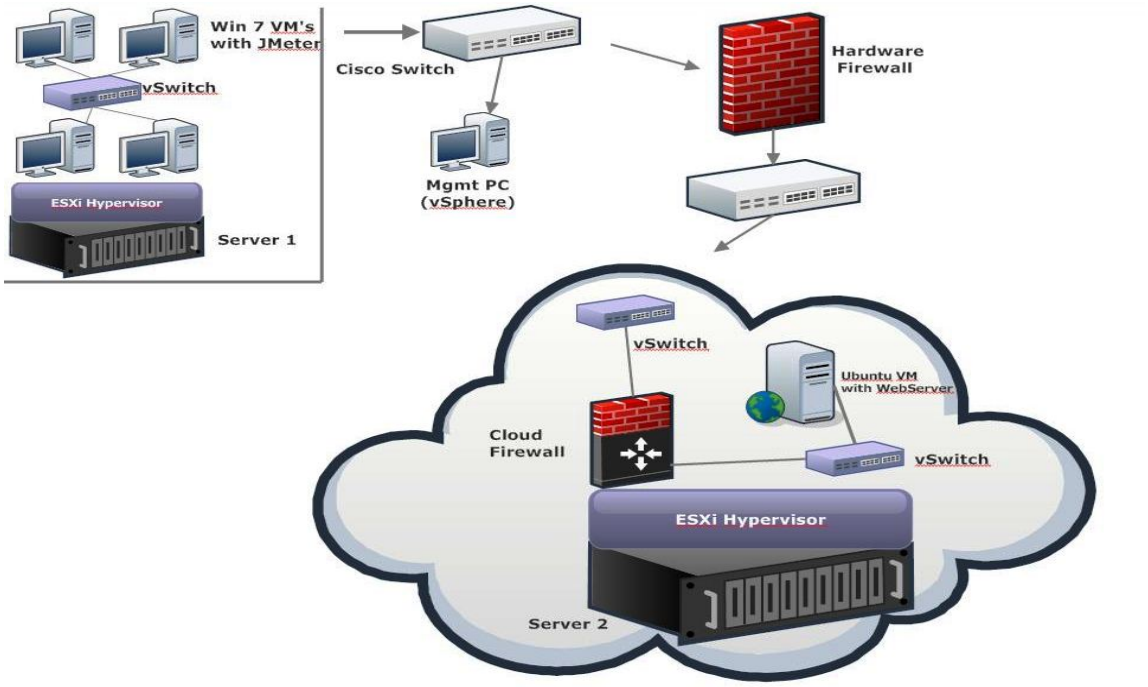


Figure 22: Federated Model

5.4 Phase II: Simulation Test

Implemented and designed to stress the devices using heavy traffic and load.

5.4.1 Test I: Federated Model

The federated model used two firewalls (Cisco ASA & Vyatta). It also used 61 standalone computers with windows 7 OS installed and 3 JMeter's masters installed on 3 of the computers, two of the JMeter's are used to send traffic, and the other JMeter is used to monitor the traffic. Another standalone computer is used with vSphere Client to monitor ESXi hypervisors, 2 Cisco switch are used to connect the network. 2 vSwitch for Vyatta and webserver, 1 ESXi hypervisor and 1 Server. A diagrammatic representation of the phase II - federated architecture is shown below: The IP addresses and subnets configurations are shown in Appendix D.

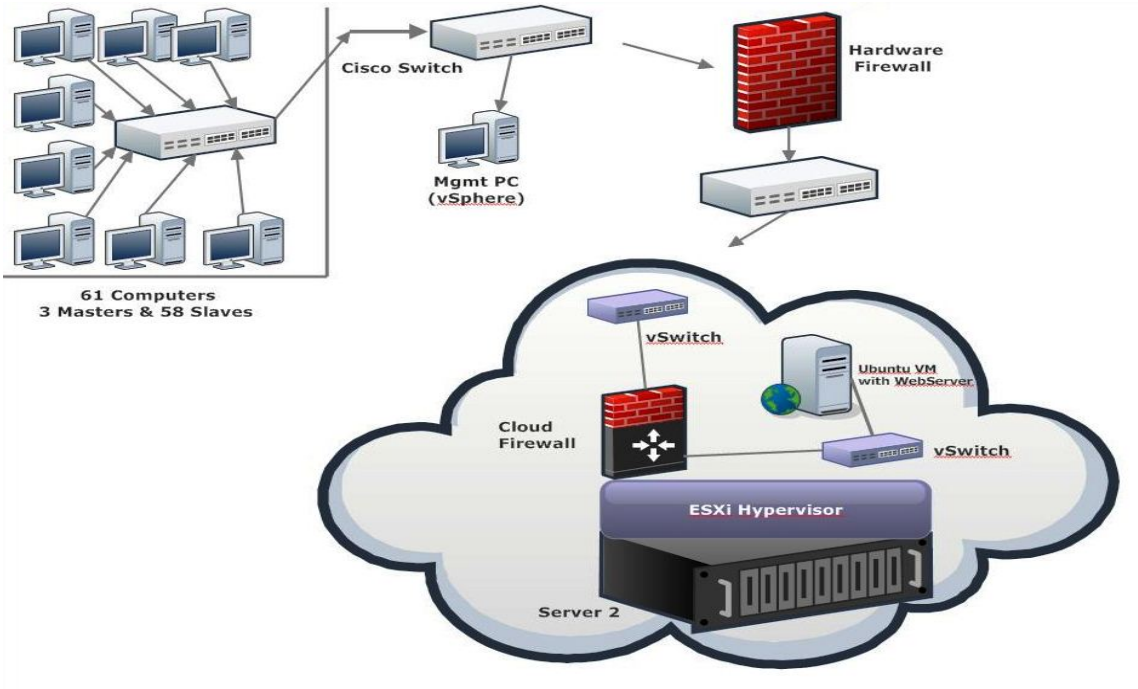


Figure 23: Phase II - Federated architecture

5.4.2 Test II: Cloud vs. Hardware Model

Hardware:

The hardware model used only the Cisco ASA firewall, with the same configuration as the federated model, but using only one vSwitch for the webserver, and Vyatta not present. A diagrammatic representation of the hardware architecture is shown below: The IP addresses and subnets configurations are shown in Appendix D. In this test, the traffic was reduced to a bearable load which the hardware firewall can handle.

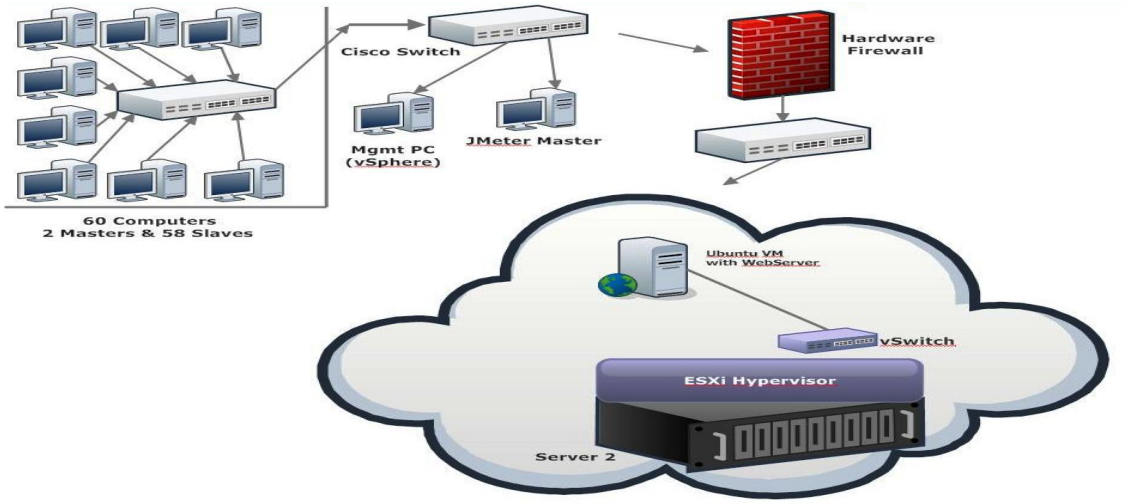


Figure 24: Phase II - Hardware Architecture

Cloud:

The cloud model used only the Vyatta cloud firewall with the same architecture like that of the federated, but using only one Cisco Switch and no Cisco ASA. A diagrammatic representation of the phase II - cloud architecture is shown below: The IP addresses and subnets configurations are shown in Appendix D.

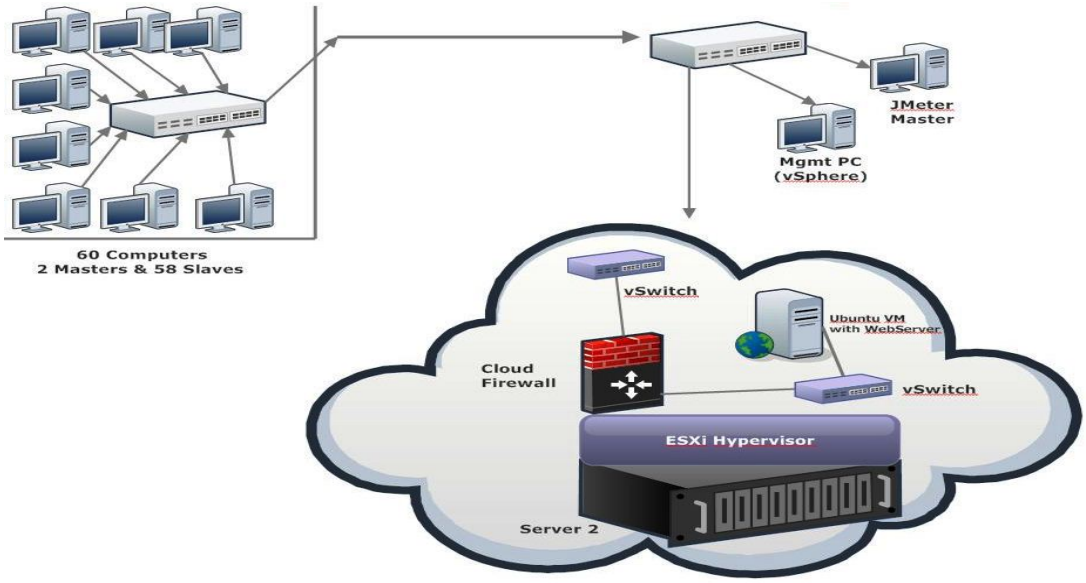


Figure 25: Phase II - Cloud Architecture

CHAPTER SIX
RESULT & ANALYSIS

6.1 Results

The results focus on the different test scenarios carried out. Endurance and spike throughput, and mathematical calculations were also used to analyze the results and compare the different models. This work has two phases, with the first being a pilot test and the second a simulation test, phase one has four different tests, and phase two has two different tests respectively. Phase II, test one, is carried with the goal of maxing out the Cisco ASA resources, and test two is carried out to compare the difference between the two types of firewalls used in this research. Each phase result is collected and carefully analyzed.

6.2 Phase I: Pilot Test Result, Analysis and Comparison

6.2.1 Spike Test

The results collected from the spike test of the different models is tabulated below:

Model	No. Of Packets	Spike Point (Pkts)	Spike Time (ms)	Last Time	Throughput (Pkts/Sec)	Avg	St.Dev	Transfer Rate (KB/Sec)
Control	9835	6000	7200	0	718.7/sec	3941	2997	372.75
Cloud	9900	9278	21022	0	427.6/sec	806	3262.8	233.1
Hardware	9699	6800	9150	0	457.2/sec	4873	3739	265.3
Federated	9900	9686	21028	15	428.0/sec	401	1745.1	222.7

Table 4: Spike Result

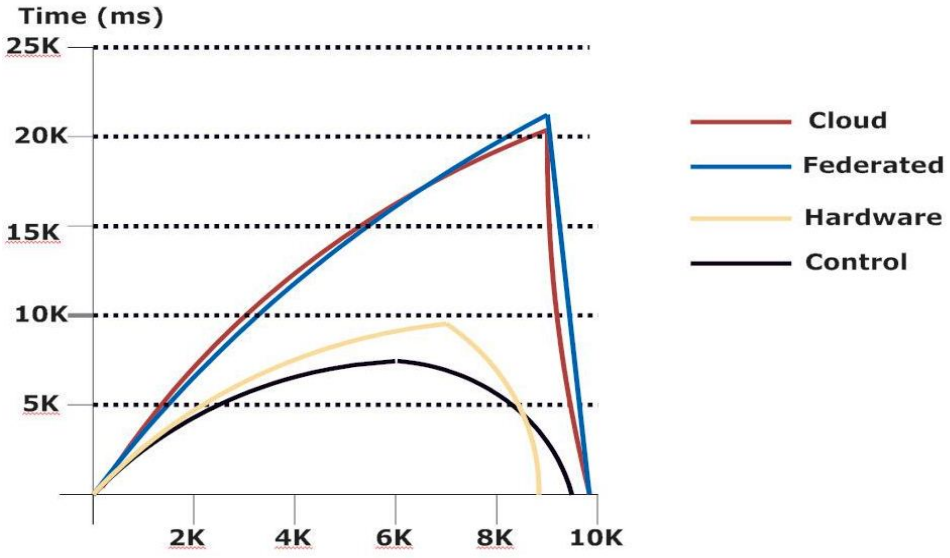


Figure 26: Spike Chart

Figure 26 shows the spike result of all the architectures in Phase I, the control architecture proves to have a better performance under test with a spike point of 6000 packets at 7.2 seconds, followed by the hardware firewall with 6800 packets at 9.15 seconds. However that of the cloud firewall took a longer period of time to reach its spike point of 9278 packets in 21 seconds. The result of the federated architecture could be attributed to the fact that the cloud firewall is incorporated in it. It also has a higher spike of 9686 packets at 21 seconds.

Figure 27 below shows a bar chart of the spike throughput results of each architecture. Considering that the control architecture has no firewall in it, therefore there is no filtering, it has a throughput of 718.7 packets per second making it the best architecture, but not secured. Also the hardware firewall proves to have a better throughput with 457.2 packets per second than the cloud at 427.6 packets per second. The difference between the two architectures shows the effect on the federated architecture

with 428.0 packets per second, which has a very small difference with the cloud architecture.

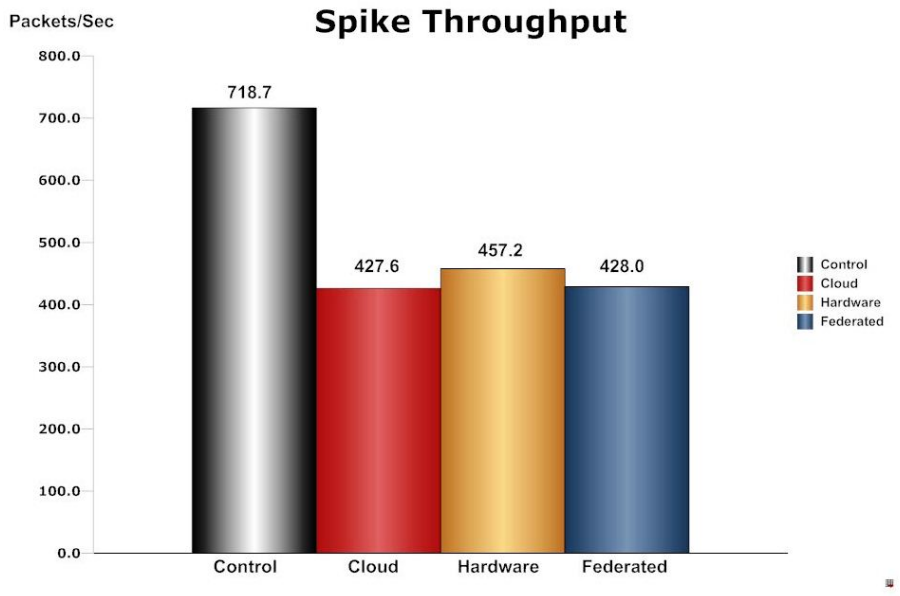


Figure 27: Spike Throughput

A T-test statistics is carried out to compare the cloud-based vs. the hardware based: The result of the test shows that there is a clear difference between the two firewalls.

Hypothesis:

Ho: There is no performance difference between the architectures: $\mu_1 = \mu_2$

Ha: There is a difference between the architectures: $\mu_1 \neq \mu_2$

For Cloud:

Average ($\ddot{X}_1$) = 806

Standard Deviation (s_1) = 3262.8

Sample (N_1) = 9900

For Hardware:

Average ($\ddot{X}_2$) = 4873

Standard deviation (s_2) = 3739

Sample (N_2) = 9699

Alpha = .05

Degrees of Freedom = $N_1 + N_2 - 2$ = (9900 + 9699)-2 = 19597

From t-table: t-critical = 1.960

Using the formula for t-test

$$t = \frac{\overline{X_1} - \overline{X_2}}{S_{\overline{x}_1 - \overline{x}_2}}$$

For unequal sample size and unequal variance:

$$s_{\overline{X}_1 - \overline{X}_2} = \sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}} = \sqrt{\frac{3262.8^2}{9900} + \frac{3739^2}{9699}} = 50.2$$

Therefore $t = \frac{\overline{X_1} - \overline{X_2}}{S_{\overline{x}_1 - \overline{x}_2}} = \frac{806-4873}{50.2} = 81$

T-critical < t-test = 1.960 < 81

We reject the null hypothesis; there is a performance difference between the architecture.

6.2.2 Endurance Test

The results collected from the endurance test of the different models in tabulated below:

Model	No. Of Packets	Time (ms)	Throughput (Pkts/Sec)	Avg	St.Dev	Transfer Rate (KB/Sec)
Control	9904	6000	579.4/sec	3014	1982	300.6
Cloud	9750	21025	428.3/sec	273	1333.2	222.9
Hardware	9796	8200	462.5/sec	4198	3816	258.2
Federated	9750	21021	377.9/sec	158	790.1	225.4

Table 5: Endurance Test Result

The two figures below, figure 28 and figure 29 shows the endurance throughput and the endurance chart of the 4 different architectures of phase I. Like that of the spike test; the control architecture proves to sustain a better continues load by delivering 9904 packets out of the 10,000 packets sent in 6seconds, followed by the control architecture is the hardware firewall delivering 9796 packets in 8.2 seconds, then the federated and cloud

architecture both delivering 9750 packets in 21 seconds, with that of the cloud a little higher by a difference of 0.004 seconds

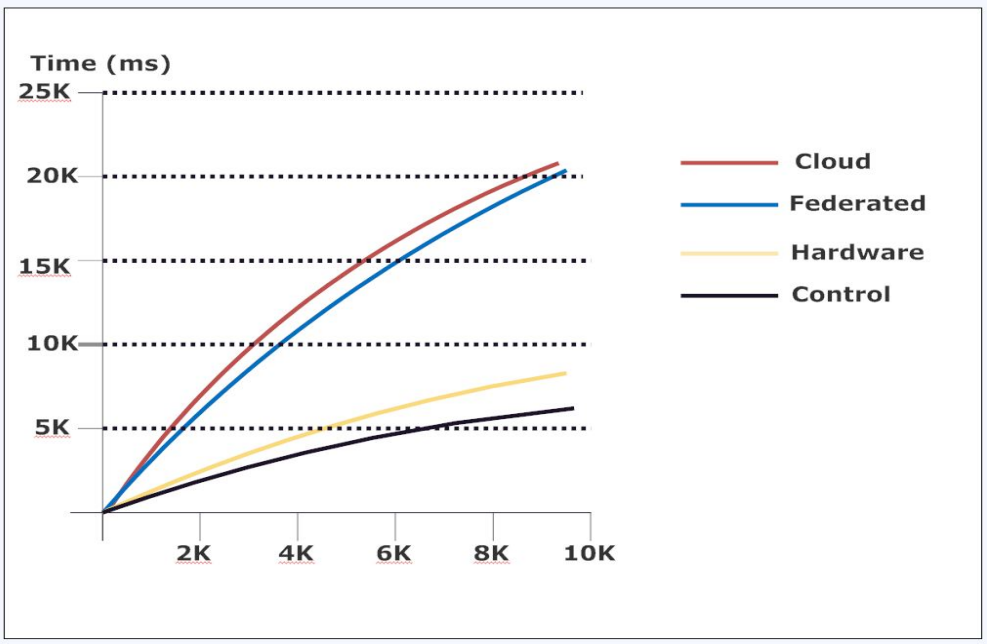


Figure 28: Endurance Chart

A bar chart below shows the throughput of each model

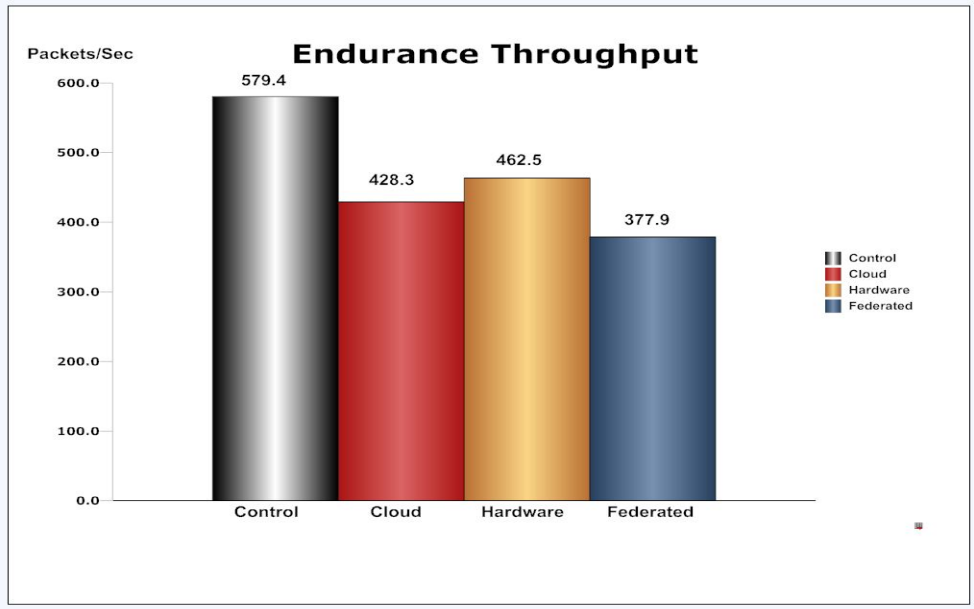


Figure 29: Endurance Throughput

A T-test statistics is carried to compare the cloud-based vs. the hardware-based. The result of the test shows that there is a significance endurance difference between the two firewalls.

Hypothesis:

Ho: There is no performance difference between the architectures: $\mu_1 = \mu_2$

Ha: There is a difference between the architectures: $\mu_1 \neq \mu_2$

For Cloud:

Average ($\ddot{X}_1$) = 273

Standard Deviation (s_1) = 1332

Sample (N_1) = 9750

For Hardware:

Average ($\ddot{X}_2$) = 4198

Standard deviation (s_2) = 3816

Sample (N_2) = 9796

Alpha = .05

Degrees of Freedom = $N_1 + N_2 - 2$ = (9750 + 9796)-2 = 19544

From t-table: t-critical = 1.960

Using the formula for t-test

$$t = \frac{\overline{X_1} - \overline{X_2}}{S_{\overline{x_1} - \overline{x_2}}}$$

For unequal sample size and unequal variance:

$$s_{\overline{X}_1 - \overline{X}_2} = \sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}} = \sqrt{\frac{1332^2}{9750} + \frac{3816^2}{9796}} = 40.8$$

Therefore $t = \frac{\overline{X_1} - \overline{X_2}}{S_{\overline{x_1} - \overline{x_2}}} = \frac{273 - 4198}{40.8} = 96$

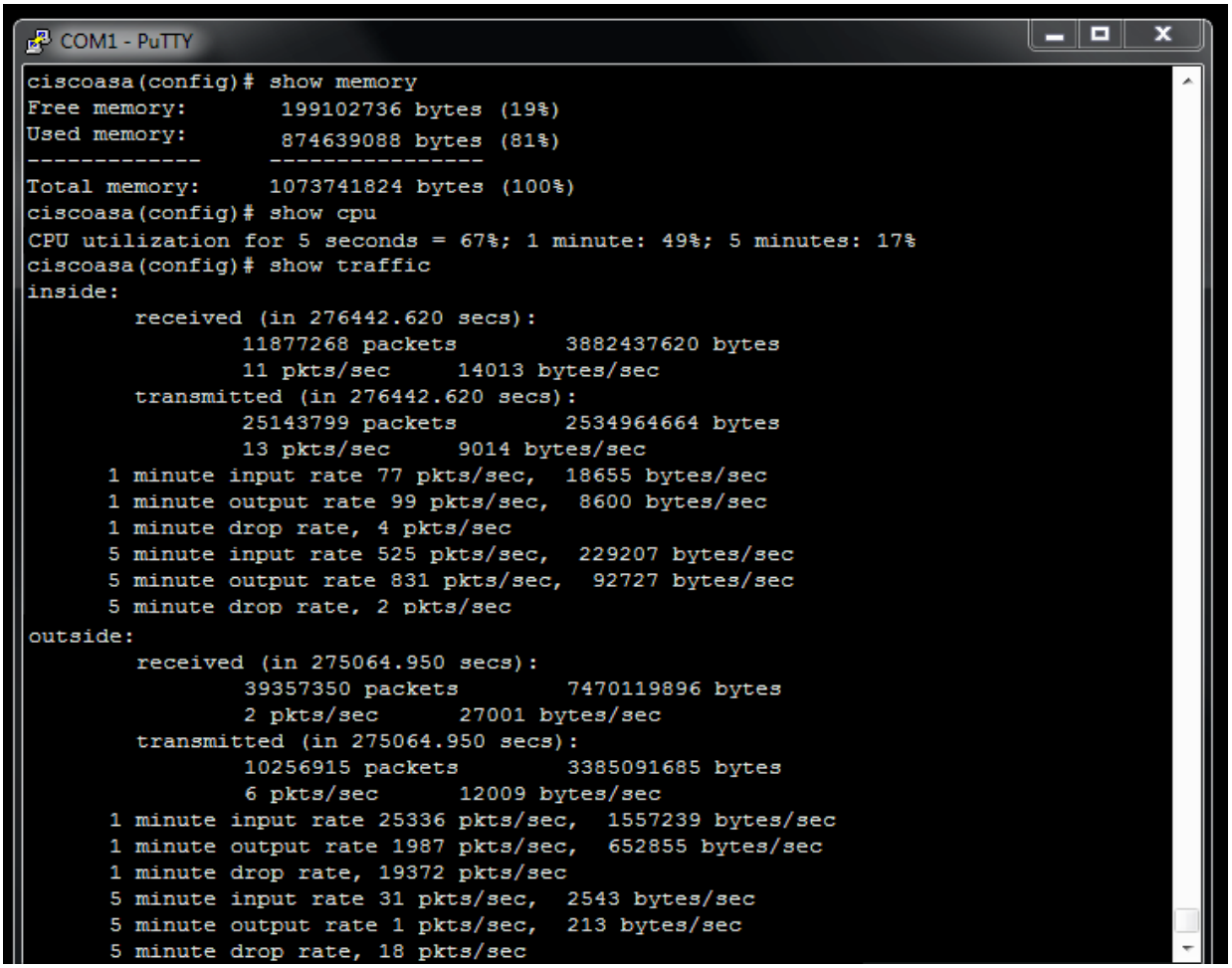
T-critical < t-test = 1.960 < 96

We reject the null hypothesis; there is a performance difference between the architecture.

6.3 Phase II: Simulation Test

6.3.1 Test One: Federated:

Screen Shot 8 below shows the exact time and the usage of the hardware resource before it completely froze and totally failed.



Screen Shot 7: Phase II – Used Hardware Resources

As seen below in figure 30, 31, 32, 33 and 34. In the simulation test which uses real traffic generated from 62 computers, the packet drop rate is at 76.5%, the CPU Utilization is at 67% while the memory is at 81%, this is the level at which the hardware firewall became non-responsive, the hardware firewall was maxed out which result to its failure completely and having a downtime of about 30 seconds. At the time the hardware firewall

failed, all other services like JMeter froze and completely stopped responding, with the exception of the cloud-firewall that continues running because it has no resources to be maxed out. Figure 33 shows the point at which the hardware firewall is responsive and non-responsive.

As a result of this, we concluded that the hardware firewall has a better performance while the cloud firewall can withstand a heavier traffic than the hardware firewall.

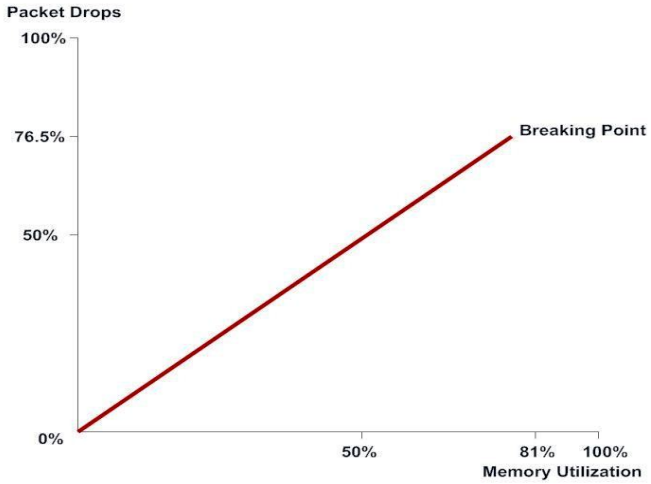


Figure 30: Hardware Packet drop vs. Memory Utilization

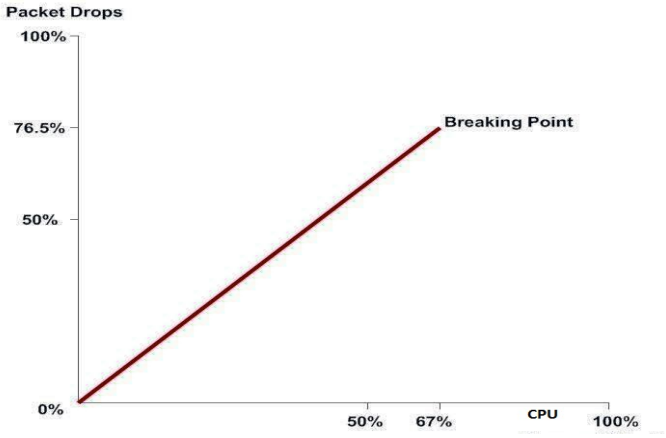


Figure 31: Hardware Packet drop vs. CPU Utilization

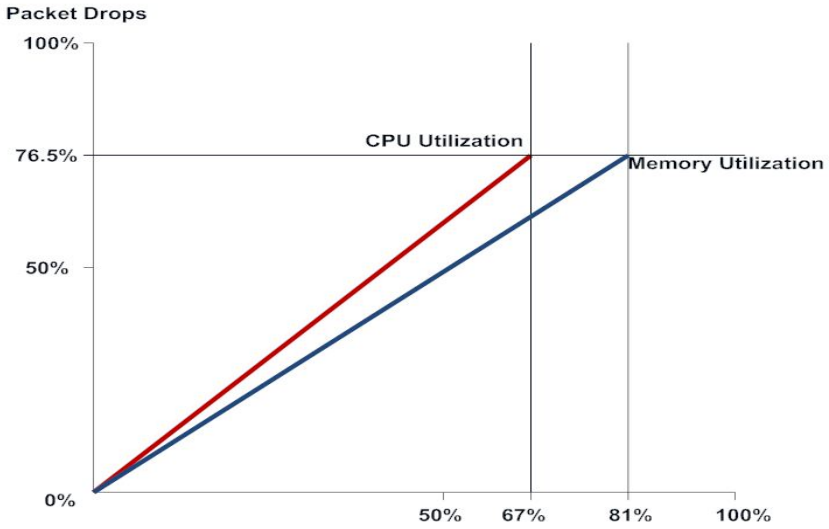


Figure 32: Hardware Packet Drops, CPU Utilization and Memory Utilization

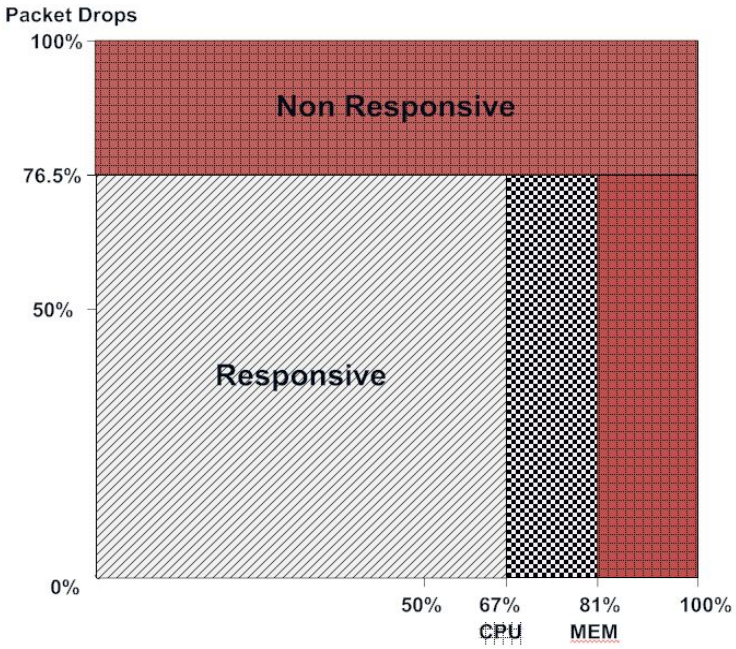


Figure 33: Hardware Packet Drops, CPU Utilization and Memory Utilization

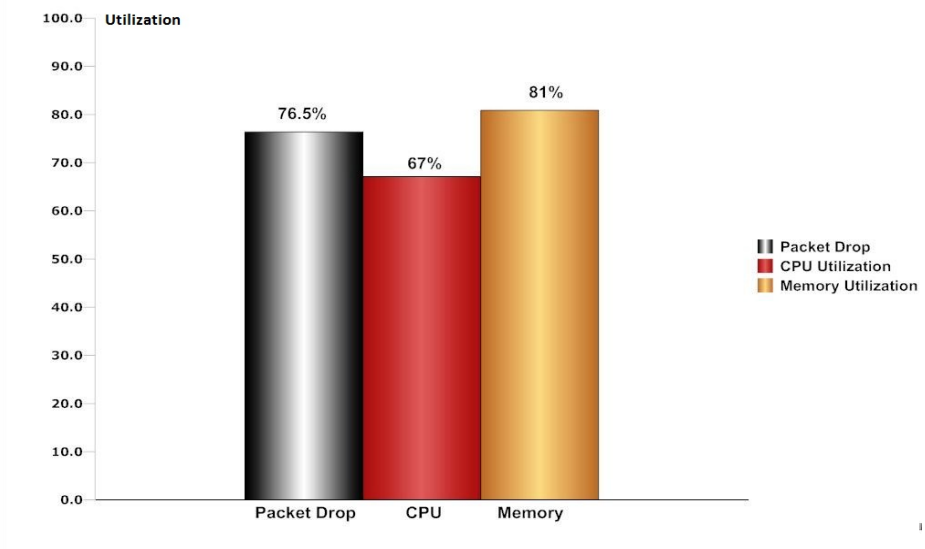


Figure 34: Hardware Packet Drops, CPU Utilization and Memory Utilization Bar Chart

6.3.2 Test Two: Hardware vs. Cloud

Model	No. of Samples	Average	St. Dev	Throughput (Pkts/Sec)
Hardware	47900	2936	8702.3	189.9/sec
Cloud	54006	453	2539.7	484.6/sec

Table 6: Phase II – Test Results

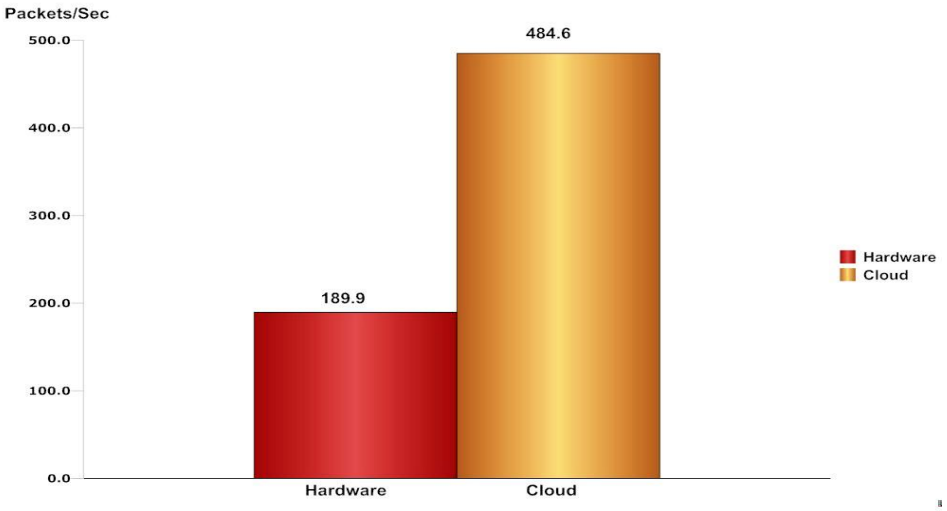


Figure 35: Throughput Result

Figure 35 above shows the throughput of both firewalls under a bearable traffic which the hardware firewall can handle, but considering that there was too much traffic and the hardware firewall was stressed and close to maxing out its resources, you can see that the throughput of the hardware firewall has decreased and is far much less than that of the cloud, this is because the resources utilized by the hardware firewall are close to being exhausted.

We did a statistical analysis of the results collected from both devices and the result is shown below mathematically:

Hypothesis:

- Ho: There is no performance difference between the architectures: $\mu_1 = \mu_2$
- Ha: There is a difference between the architectures: $\mu_1 \neq \mu_2$

For Cloud:

Average ($\ddot{X}_1$) = 453

Standard Deviation (s_1) = 2539.7

Sample (N_1) = 54006

For Hardware:

Average ($\ddot{X}_2$) = 2936

Standard deviation (s_2) = 8702

Sample (N_2) = 47900

Alpha = .05

Degrees of Freedom = $N_1 + N_2 - 2$ = (54006 + 47900)-2 = 101904

From t-table: t-critical = 1.960

Using the formula for t-test

$$t = \frac{\overline{X_1} - \overline{X_2}}{S_{\overline{x_1} - \overline{x_2}}}$$

-

For unequal sample size and unequal variance:

$$s_{\overline{X}_1 - \overline{X}_2} = \sqrt{\frac{s_1^2}{n_1} + \frac{s_2^2}{n_2}} = \sqrt{\frac{2539.7^2}{54006} + \frac{8702^2}{47900}} = 41$$

Therefore $t = \frac{\overline{X_1} - \overline{X_2}}{S_{\overline{x_1} - \overline{x_2}}} = \frac{453 - 2936}{41} = 61$

T-critical < t-test = 1.960 < 61

We reject the null hypothesis; there is a performance difference between the architecture.

6.4 New Thresholds & Filter Decision Flow

Considering the fact that the hardware firewall fails under heavy traffic while the cloud firewall is still running, we decided to define and set a new thresholds. When these thresholds are reached, the device is rendered incapable of performing as required:

6.4.1 Max Defined Thresholds (S.L.A)

Packet drop => 10%

Memory Utilization => 80%

CPU Utilization => 65%

If this thesis is to be implemented in an organization, the thresholds can be defined based on Service Level Agreements (S.L.A)

6.4.2 Heuristics Rules

For the purpose of this thesis, the proposed heuristics rules (conditions) that define the migration from hardware to the cloud are listed below:

1. If $Pd is high then $MgC else $ContH
2. If $Tp is low, then $MgC else $ContH
3. If $CPUU is high then $MgC else $ContH
4. If $MemU is high the $MgC else $ContH
5. If $Scen1 is null then $ContH else $MgC

Heuristics Acronyms:

Migrate to Cloud = MgC

Continue on Hardware = ContH

Throughput = Tp

CPU Utilization	=	CPUU
Memory Utilization	=	MemU
Scenario 1	=	Scen1
Packet Drop	=	Pd

Heuristics Definition:

1. If $Pd is high then $MgC else $ContH

   The rule states that if the packet drops ($Pd) is high then migrate to cloud ($MgC) else continue to hardware ($ContH).

2. If $Tp is low, then $MgC else $ContH

   If the throughput is extremely low, then migrate to the cloud else continue on hardware.

3. If $CPUU is high then $MgC else $ContH

   If the CPU Utilization is high then migrate to optimize performance and resources.

4. If $MemU is high then $MgC else $ContH

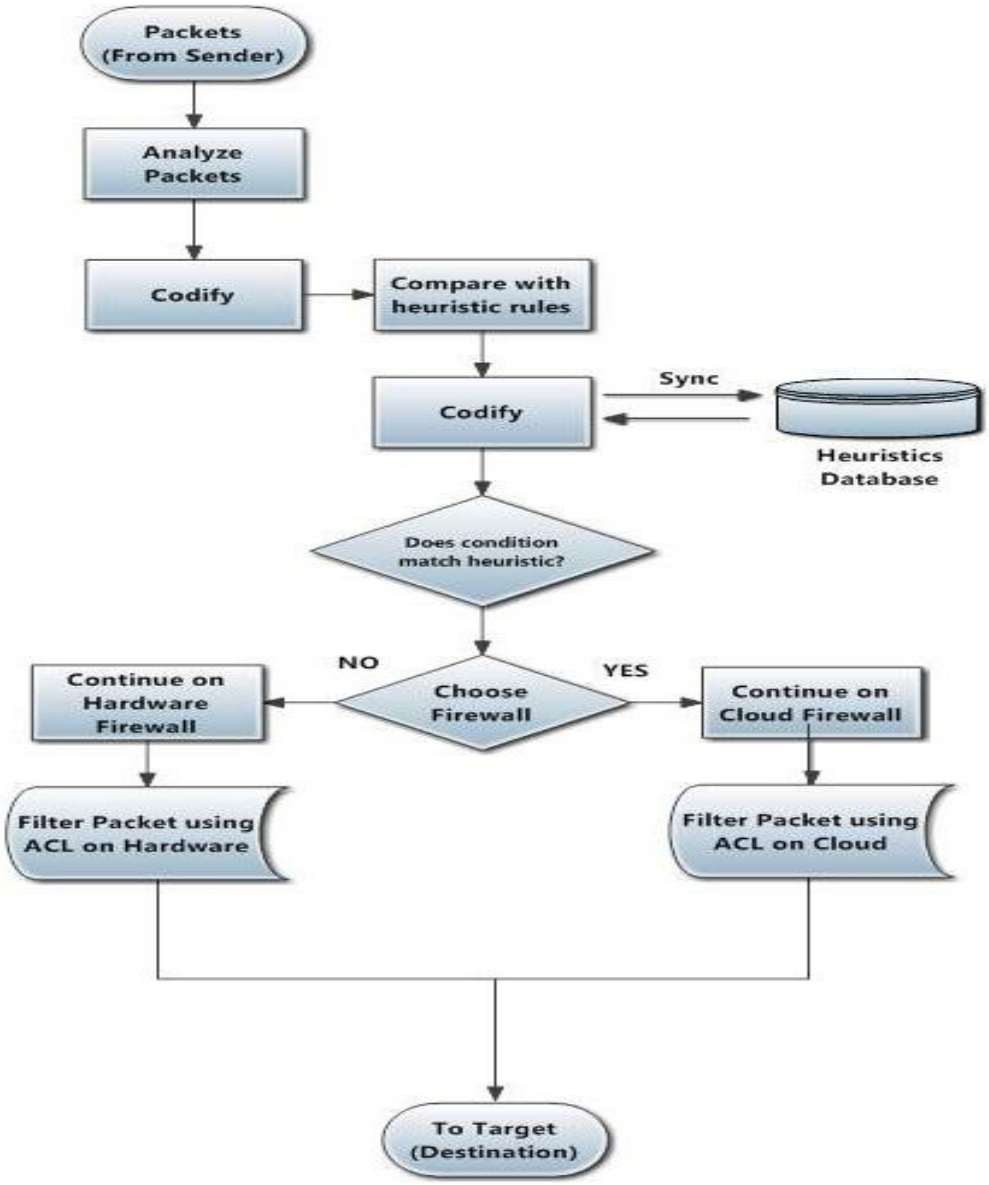
   If Memory Utilization is high then migrate to cloud else continue on hardware.

5. If $Scen1 is null then $ContH else $MgC

   If none of the conditions in Scenario 1 is met, then filtering should continue on hardware.

6.4.3 Filter Point Decision Process Flow:

How packet flows and decision made under the heuristics rules above on whether the packet should be filtered on the cloud firewall or hardware firewall is shown on the flow chart below:



Flow Chart 1: Filter Point Decision

CHAPTER SEVEN
CONCLUSION

7.1 Discussion and Conclusion

Two different types of firewall, one is a hardware-based and the other a cloud-based have undergone a series of different types of test. They have been tested individually, and also together. Two scenarios had been used to make decisions on the outcome, which are endurance and spike test. Also throughput and mathematical calculations were used to compare the different devices.

The work is based two different phases; Phase One has four different tests; control, cloud-based, hardware-based and federated. Phase Two has two different test, federated test and cloud-based vs. hardware-based.

Based on the test results and analysis, it is proved that the hardware firewall has a better performance at normalized traffic than the cloud firewall, but under a heavy traffic, the cloud firewall proves to beat the hardware firewall due to the fact that the cloud firewall has no resources to be utilized, while the hardware firewall does.

7.2 Recommendation & Future Work

From this study, certain recommendation can be followed in other to optimize security and performance of firewalls in networks. The evaluations of the firewall systems include many aspects depending on the memory utilization, CPU utilization, packet drops, and available resources. Especially with the hardware, the resources used in this work might be much better or much lesser than that required by another organization, so

therefore deciding on threshold and heuristic rules to be used to migrate service to the cloud solemnly depends on the resources available and needs of an institution. This could be decided based on service user agreement (S.L.A). This work is just a lay out of how decision and work can be carried out.

Future work can focus on different parts depending on needs, some of which could be:

- What is the weakness of the cloud-based firewall compared with hardware-based and how can we use that to optimize the architecture.
- How can we migrate service to the hardware-based firewall and under what conditions?
- Develop a heuristic list for migration to hardware due to constraints on the cloud.
- Exploit the weakness of the cloud.
- Any idea on how to optimize the performance of this test could be a future work.

REFERENCES

Acharya, S., Wang, J., Ge, Z., Znati, T.F., & Greenberg, A., "Traffic-Aware Firewall Optimization Strategies." Communications, ICC '06 IEEE International Conference. Vol: 5 pp 2225-2230. 2006.

Adams, K., & Agesen, Ole., "A Comparison of Software and Hardware Techniques for x86 Virtualization" *ASPLOS XII Proceedings of the 12th International Conference on Architectural support for programming languages and operating systems.* pp. 2-13 (2006).

Apache., "Apache JMeter" 2013. *The Apache Software Foundation* (accessed November 11th, 2013) jmeter.apache.org.

Apache., "Remote Testing" 2013. *The Apache Software Foundation* (accessed November 11th, 2013) jmeter.apache.org/usermanual/remote-test.html.

Basak, D., Toshniwal, R., Maskalik, S., & Sequeria, A., "Virtualizing Networking and Security in the Cloud" *Newsletter ACM SIGOPS.* (2010) Vol: 44 no. 4 pp 86-94.

Blancharski, D., *Network Security in a Mixed Environment.* Foster City, CA: IDG Books Worldwide, 1998.

Buyya, R., Broberg, J., and Goscinski, A.M., *Cloud Computing: Principles and Paradigms.* New York, NY: Wiley, 2011.

Cisco., *What is a Network Switch vs. a Router?* 2014 (accessed on Feb 8th, 2014) http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/what_is_a_network_switch/index.html

Cisco. *What is Network Security?* 2014 (accessed Feb13th, 2014) http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html

CSA, "Top Threats to Cloud Computing v1.0" *Cloud Security Alliance.* 2010 (accessed Feb 12th, 2014) https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing v2.1" *Cloud Security Alliance.* 2009 (accessed Feb 12th, 2014) https://cloudsecurityalliance.org/csaguide.pdf

Forouzan, B.A., *Business Data Communications.* New York, NY: McGraw-Hill, 2003.

Funke, R., Grote, A., & Heiss, H., "Performance Evaluation of Firewalls in Gigabit-Networks." 2002.

Guillen, E., Sossa, A.N., & Estupinan, E.P., "Performance Analysis over Software Router vs. Hardware Router: A practical Approach" *Proceedings of the World Congress on Engineering and Computer Science.* 2012 Vol. II.

Lammle, T., *Cisco Certified Network Associate Study Guide.* Indianapolis, IN: Wiley, 2011.

Lyu, M.R., & Lau, L.K.Y., "Firewall Security: Policies, Testing and Performance Evaluation." *Computer Software and Applications Conference.* ISSN:0730-3157, pp. 116-121 (2000).

Mell, P., and Grance, T., "The NIST Definition of Cloud Computing" *Special Publication 800-145,* 2011: pp. 2-3. (accessed Feb 13th, 2014) http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Nakrem, A., "Managing Information Security in Organizations: A case study." *Master's Thesis* 2007.

NSTISSC., “National Information Systems Security (Info Sec) Glossary” 2000 (NSTISSC 2000)

Panko, R.R., *Corporate Computer and Network Security.* Upper Saddle River, NJ: Pearson Education, 2003.

Popek, J.G., “Formal Requirements for Virtualizable Third Generation Architectures.” *Communications of the ACM.* Vol 17, no. 7 (1974).

Regan, P., *Local Area Networks.* Columbus, OH: Pearson Prentice Hall, 2004.

Ricciuti, M., “Next version of Windows*:* Call it 7*”.* 2007 *CNET News Operating Systems* (accessed on Feb 20th, 2014) http://news.cnet.com/2100-1016_3-6197943.html

Robin, J.S., and Irvine, C.E., “Analysis of Intel Pentium’s Ability to Support a Secure Virtual Machine Monitor” Center for Information System Studies and Research Computer Sciences Department Naval Postgraduate School. Monterey, CA, 2000.

Sheth, C., & Thakker, R., “Performance Evaluation and Comparative Analysis of Network Firewalls” *IEEE.* 2011.

Sheth, C., & Thakker, R., “Performance Evaluation and Comparison of Network Firewalls under DDoS Attack” I.J Computer Network and Information Security. 2013, 12, 60-67.

Su, W., & Xu, J., “Performance Evaluations of Cisco ASA and Linux IPTables Firewall Solutions” *Master’s Thesis* 2013.

Subashini, S., & Kavitha, V., “A survey on security issues in service delivery models of cloud computing” *Journal of Network and Computer Applications.* 1084-8045 (2010).

Tetteywayo, A.N., and Akpabi, W.Y., “Securing the Linux Web Server via the Linux Netfilter/IPTable Firewall.” *Master’s Thesis* 2012.

Thomas, T., *Network Security First-Step*. Indianapolis, IN: Cisco Press, 2004.

Vyatta., *Vyatta System Firewall Reference Guide.* Belmont, CA: (2012) (retrieved on Feb 7th, 2014) https://54712289bdd910def82d-5cc7866f7aae0a382278b5bce7412a4a.ssl.cf1.rackcdn.com/Vyatta-Firewall_6.5R1_v01.pdf

APPENDIX A

VYATTA FIREWALL RULES

Rule 1:

Vyatta# set firewall name FWRULES-1 rule 1 action reject

Vyatta# set firewall name FWRULES-1 rule 1 source address 172.16.10.2

Vyatta# set firewall name FWRULES-1 rule 1 protocol TCP

Rule 2:

Vyatta# set firewall name FWRULES-1 rule 2 action reject

Vyatta# set firewall name FWRULES-1 rule 2 source address 18.102.0.0

Vyatta# set firewall name FWRULES-1 rule 2 protocol TCP

Rule 3:

Vyatta# set firewall name FWRULES-1 rule 3 action reject

Vyatta# set firewall name FWRULES-1 rule 3 protocol UDP

Vyatta# set firewall name FWRULES-1 rule 3 destination port 520

Rule 4:

Vyatta# set firewall name FWRULES-1 rule 4 action reject

Vyatta# set firewall name FWRULES-1 rule 4 source address 120.147.60.0

Vyatta# set firewall name FWRULES-1 rule 4 protocol IP

Rule 5:

Vyatta# set firewall name FWRULES-1 rule 5 action reject

Vyatta# set firewall name FWRULES-1 rule 5 protocol OSPF

Rule 6:

Vyatta# set firewall name FWRULES-1 rule 6 action reject

Vyatta# set firewall name FWRULES-1 rule 6 source address 101.22.34.1

Vyatta# set firewall name FWRULES-1 rule 6 protocol TCP

Rule 7:

Vyatta# set firewall name FWRULES-1 rule 7 action accept

Vyatta# set firewall name FWRULES-1 rule 7 protocol TCP

Vyatta# set firewall name FWRULES-1 rule 7 destination port 80

Rule 8:

Vyatta# set firewall name FWRULES-1 rule 8 action reject

Vyatta# set firewall name FWRULES-1 rule 8 protocol TCP

Vyatta# set firewall name FWRULES-1 rule 8 destination port 21

Rule 9:

Vyatta# set firewall name FWRULES-1 rule 9 action reject

Vyatta# set firewall name FWRULES-1 rule 9 protocol TCP

Vyatta# set firewall name FWRULES-1 rule 9 destination port 22

Rule 10:

Vyatta# set firewall name FWRULES-1 rule 10 action reject

Vyatta# set firewall name FWRULES-1 rule 10 protocol TCP

Vyatta# set firewall name FWRULES-1 rule 10 destination port 25

Rule 11:

Vyatta# set firewall name FWRULES-1 rule 11 action reject

Vyatta# set firewall name FWRULES-1 rule 11 protocol TCP

Vyatta# set firewall name FWRULES-1 rule 11 destination port 110

Rule 12:

Vyatta# set firewall name FWRULES-1 rule 12 action reject

Vyatta# set firewall name FWRULES-1 rule 12 protocol TCP

Vyatta# set firewall name FWRULES-1 rule 12 destination port 143

Rule 13:

Vyatta# set firewall name FWRULES-1 rule 13 action reject

Vyatta# set firewall name FWRULES-1 rule 13 protocol UDP

Vyatta# set firewall name FWRULES-1 rule 13 destination port 135

Rule 14:

Vyatta# set firewall name FWRULES-1 rule 14 action reject

Vyatta# set firewall name FWRULES-1 rule 14 protocol TCP

Vyatta# set firewall name FWRULES-1 rule 14 destination port 445

Rule 15:

Vyatta# set firewall name FWRULES-1 rule 15 action reject

Vyatta# set firewall name FWRULES-1 rule 15 protocol TCP

Vyatta# set firewall name FWRULES-1 rule 15 destination port 1434

Rule 16:

Vyatta# set firewall name FWRULES-1 rule 16 action reject

Vyatta# set firewall name FWRULES-1 rule 16 protocol TCP

Vyatta# set firewall name FWRULES-1 rule 16 destination port 4444

Rule 17:

Vyatta# set firewall name FWRULES-1 rule 17 action reject

Vyatta# set firewall name FWRULES-1 rule 17 protocol TCP

Vyatta# set firewall name FWRULES-1 rule 17 destination port 4899

Rule 18:

Vyatta# set firewall name FWRULES-1 rule 18 action accept

Vyatta# set firewall name FWRULES-1 rule 18 protocol ICMP

Rule 19:

Vyatta# set firewall name FWRULES-1 rule 19 action accept

Vyatta# set firewall name FWRULES-1 rule 19 source address 192.168.0.0

Vyatta# set firewall name FWRULES-1 rule 19 protocol TCP

Rule 20:

Vyatta# set firewall name FWRULES-1 rule 20 action accept

Vyatta# set firewall name FWRULES-1 rule 20 protocol TCP

Vyatta# set firewall name FWRULES-1 rule 20 destination address 120.147.60.3

Apply to interface and commit:

Vyatta# set interfaces ethernet eth1 firewall in name FWRULES-1

Vyatta# commit

To show firewall:

Vyatta# show firewall name FWRULES-1

To show firewall on interface:

Vyatta# show interfaces ethernet eth1 firewall

APPENDIX B

CISCO ASA FIREWALL RULES

1. Config# access-list 110 deny tcp any host 172.16.10.2
2. Config# access-list 110 deny tcp any host 18.102.0.0
3. Config# access-list 110 deny udp any any eq 520
4. Config# access-list 110 deny ip any host 120.147.60.0
5. Config# access-list 110 deny ospf any any
6. Config# access-list 110 deny host 101.22.34.1
7. Config# access-list 110 permit tcp any any eq 80
8. Config# access-list 110 deny tcp any any eq 21
9. Config# access-list 110 deny tcp any any eq 22
10. Config# access-list 110 deny tcp any any eq 25
11. Config# access-list 110 deny tcp any any eq 110
12. Config# access-list 110 deny tcp any any eq 143
13. Config# access-list 110 deny udp any any eq 135
14. Config# access-list 110 deny tcp any any eq 445
15. Config# access-list 110 deny tcp any any eq 1434
16. Config# access-list 110 deny tcp any any eq 4444
17. Config# access-list 110 deny tcp any any eq 4899
18. Config# access-list 110 permit icmp any any
19. Config# access-list 110 permit tcp any host 192.168.0.0
20. Config# access-list 110 permit tcp any host 120.147.60.3

Apply to inbound traffic on ethernet0/0 (outside interface)

1. Config# access-group 110 in interface outside

APPENDIX C

CONFIGURING CISCO ASA FOR TRANSPARENT MODE

- Enter configuration mode
- Set to transparent = “firewall transparent”
- Configure interfaces don’t assign IP’s, give names & security level
    - “int eth0/0”
    - “no shut”
    - “nameif inside”
    - “security-level 100”
    - “int eth0/1”
    - “no shut”
    - “nameif outside”
    - “security-level 0”
- Configure management interface, no IP’s, give name & security level
    - “int management0/0”
    - “no shut”
    - “nameif management”
    - “security-level 50”
- Assign a global IP address (should be in the same subnet).
    - “ip address 10.10.10.70 255.255.255.0”
- Apply ACL
- Save configuration:
    - “copy running-config startup-config”

APPENDIX D

IP ADDRESSES & SUBNETS

Subnet /24

IP = 10.10.10.X

Device	IP/Subnet
Server One: Web Server	.20/24
Vyatta (eth 0)	.60/24
Vyatta (eth 0)	.61/24
Ubuntu Web Server	.54/24
Server Two: JMeter	.21/24
JMeter Master	.50/24
JMeter Slave 1	.51/24
JMeter Slave 2	.52/24
JMeter Slave 3	.53/24
Cisco ASA:	
Interface 0/0 & 0/1	Transparent Interfaces
Global IP	.70/24
Standalone Computers:	
Management PC	.22/24

3 JMeter Masters	.24/24 , .25/24 , .26/24
22 JMeter Slaves	.27 to .49/24
26 JMeter Slaves	.70 to .95 /24
10 JMeter Slaves	.101 to .110/24