# MEASURING NETWORK PERFORMANCE WITH DIFFERENT LEVELS OF FIREWALL SECURITY

By

**RICHMOND ADUSEI (BSc. Computer Science)**

A Thesis submitted to the School of Graduate Studies, Kwame Nkrumah University of Science and Technology in partial fulfillment of the requirement for a Master's Degree in

**INFORMATION TECHNOLOGY**

**JUNE, 2016**

## DECLARATION

I hereby declare that this thesis is my own work towards the MSc. degree and that to the best of my knowledge it contains no material previously published by another person nor material which has been accepted for the award of any other degree of any University, except where due reference has been made in the text.

| | | |
|---|---|---|
| RICHMOND ADUSEI | …… | …… |
| (PG8296912) | Signature | Date |

Certified by:

| | | |
|---|---|---|
| Mr. Dominic Asamoah | …… | …….. |
| Supervisor's | Signature | Date |

| | | |
|---|---|---|
| Dr. J.B Hayfron- Acquah | ..…….. | ……... |
| Head of Department | Signature | Date |

## DEDICATION

This thesis is dedicated to my dear mother; Hagar Osei (Director, “Hagar Nyame na Aye Enterprise”), my son Nana Ampofo Adusei, my siblings Samson Owusu, Kwasi Amponsah (Multi Credit Savings and Loans Ltd), Joshuah Boateng (Kwame Nkrumah University of Science and Technology) and Mandy Boateng (St. Louis Senior High School), for their immense support and encouragement.

Also to my very good friends Steven Yamoah (Access Bank Ghana Ltd) and Enoch Okoh Kofi(American Towers). All for their encouragement and support.

## ACKNOWLEDGEMENT

I wish to give maximum thanks to the Almighty God for giving me knowledge, protection and guidance throughout this research.

Mr. Dominic Asamoah has been the ideal thesis supervisor who though entangled with a lot of schedules spent much of his precious time reading through the scripts and making the necessary corrections and relevant suggestions. His advice, insightful criticisms and patient encouragement aided the writing of the thesis in innumerable ways.

I would also like to express my profound gratitude to my family for their prayers and support; being it cash and in kind.

Finally, I wish to thank all and sundry whose assistance contributed to the success of this project work, may the good Lord richly bless you all.

## ABSTRACT

The experiment was performed to ascertain application performances on the network with different levels of protection over Wide Area Network (WAN). In order to access related applications over the cloud there must be an internet connectivity to assist the network to reach their servers remotely for the various applications deployed over the network. The networking devices such as routers are configured via Open Shortest Path First (OSPF) routing protocol to reduce utilization, ensure load sharing over the network and also to interconnect Local Area Network (LAN). In this research three scenarios are modeled with or without protection. The level of protection used was firewall to filter and block some applications and their performance is measured. Sixty workstations are used in the simulation which all accesses the database FTP and HTTP server under different scenarios. The relationship between network security and performance are estimated which include the effects of protection such as firewalls on network performance. Various scenarios were evaluated through simulations using Riverbed Modeler Academic Edition 17.1 to show the effects of different levels of protection on a network using firewalls. The results show that protecting a network with firewall directly relates to network performance for all applications. Also blocking HTTP application reduces the load on the network for better network performance.

## TABLE OF CONTENTS

**Contents** **Pages**

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ACRONYMS

| | |
|---|---|
| ARPANET | Advanced Research Project Agency Network |
| CPU | Central Processing Unit |
| DDoS | Distributed Denial of Service |
| DEC | Digital Equipment Corporation |
| GRE | Generic Routing Encapsulation |
| IBM | International Business Machine |
| IDES | Intrusion Detection Expert System |
| IDS | Intrusion Detection System |
| IPS | Intrusion Protection System |
| IPSec | Internet Protocol Security |
| L2TP | Layer 2 Tunelling Protocol |
| LAN | Local Area Network |
| Mbps | Megabits per seconds |
| MPLS | Multi-Protocol Layer Switch |
| MS-CHAP | Microsoft version of the Challenge Handshake Authentication Protocol |
| PARC | Palto Alto Research Center |
| PPTP | Point to Point Tunelling Protocol |
| RADIUS | Reduce Authentication Dail-In User Service |
| SEAL | Secure External Access Link |
| SSL | Secure Socket Layer |
| VITO | Vehicle Inspection and Technical Center |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |

# CHAPTER ONE

# INTRODUCTION

## 1.1 Introduction

The exponential growth of networks has made them complex and mission critical, creating new challenges to those who run and manage them (Bhaiji, 2008). It is normally stated that “complexity is the enemy of security". In a complex network, security rules are obtained from many different inputs. For instance, an institution is most expected to have a corporate security principle whereas each branch may have specific security rules. Human resources department also may perhaps apply specific accessibility rules for other categories of users. In an entire network, the need for integrating these whole rules can lead to inconsistencies and conflicts(Behringer, 2011).

To ensure network security predictability is very essential. A network becomes less predictable as it becomes more complicated and the possibility that negligence may result in security vulnerabilities. While specific levels of complexity are inescapable to reach a satisfactory secured state, too much complexity can cause conflict which in turn opposes the network security thus a less secured network (Behringer, 2011). The driving force for integrated network infrastructure which comprises of audio, video, pictures graphics text and thus all in one service is actually obvious, but these precipitous increasing technologies produce new security matters. Therefore, as network managers make effort to incorporate the newest technologies in their network infrastructure, network security has turned out to be a key function in building and managing today’s modern fast growing networks (Bhaiji, 2008).

Data networks are presently the usual place for every class of organization from Small- Medium Enterprises to large international companies. While the goal for using data network has remained basically the same as sharing of resources, it now incorporates sharing of information too. Organizations in the 21st century have understood that to gain and maintain competitive edge, it is very necessary to maintain free flow of information inside an organization. However, any leakage of information to their immediate competitors could be devastating, from a business perspective (Whitman and Mattord, 2012).

This need to protect information has driven many organizations to contemplate seriously on providing security for their network infrastructure. These organizations do not deal only with data protection from competitors, but also deals with threats and attacks on their networks, from curious snoopers.

With the growing reliance on networks to facilitate efficient communication and yield greater output, Information Technology industry should be more attentive to the possible security threats that can compromise network security and cause damages. Organizations in turn maximize their network security. This research measures the performances of applications on the network when there is a change in security.

To make networks secured it is important to understand what a network is, the components that formulate a network as well as network security. In brief, a network may be described as interconnection of autonomous nodes which are physically separated. These interconnected nodes may be routers, servers, switches, firewalls etc.

On the other hand, Network Security is an act of employing preventative measures which include physical and software measures to protect the underlying network infrastructure from

unauthorized access, misapplication, breakdown, alteration, damage, or inappropriate disclosure, thereby setting up a secured platform for users, hardware and software, to execute their permitted key task within a safe environment (King, 2002).

Network architecture is a conceptual framework that explains the way in which data and information are transferred from one computer to another computer considering different layers within an organization (Reeshil,2011). Precisely, Network Architecture is the complete structure of an organization's network. The network architecture model depicts a complete pictorial view of the set up network with in depth view of the entire resources available. The resources consist of hardware components designed for the connection, types of cables and devices, network design and topologies, physical and wireless connections, application areas and forthcoming strategy. Additionally, the software protocols as well as procedures buildup to network architecture. Network administrators in collaboration with network engineers and other design engineers are always responsible for designing the network architecture.

The fact here is that anytime there is a wired or wireless network connection, there are possibilities of threats. Most people are easily discouraged to establish a home or office network with the concern that information stored on hard disk may perhaps be accessed by colleagues or hackers. Possible threats to network security are always evolving. Therefore the fundamental goal for all network administrators is to ensure continuous computer network system monitoring and security (Computer Services Group, 2016). If the network security is compromised, it could lead to severe consequences, such as invasion of privacy and pilfering of information. In securing networks, the principal interest is to make sure connections being wired or wireless is protected against unauthorized access.

Network performance on the other hand refers to measures of service quality of a network as perceived by the customer.

Today, several business transactions are made through the internet. However, with the growth of mobile commerce and wireless networks it has become mandatory that security solutions become perfectly integrated, more understandable and adaptable (Computer Services Group, 2016).

### 1.2 Background Study

The Internet and the functional network protocols were created with no security in intent. Computer criminals mostly known as hackers had a great deal of prospects by exploiting the network and software insecurities. Presently, cyber security which incorporates internet, network, and software security is one of the leading areas in computer and information technology.

Since the commencement of computer networks, security has been a major concern. Until the 1990s, networks were relatively scarce and the internet was not heavily used by people. During these times, security was not considered as critical as it is today. However, with progressive inception of important and sensitive information on networks, the need arises (Danscourses, 2013).

Early, scientist with access to the internet adored performing tricks on each other through the use of networks. These tricks were safe and risk-free, but eventually, uncovered shortcomings in the security technologies of the ARPANET. During this period, the network covered a small geographical area and many users understood each other within their expertise profession. This restricted and limited the threats (Radware solutions, 2012).

Hacking and other malicious attacks such as viruses has been a serious problem for small, large and medium companies who use the network especially internet. A study conducted by The Computer Security Institute in 2009 discovered that, up to 64 percent of organizations that partook in the study were infected with malware, whereas about 14 percent of systems were penetrated by outsiders. Each of these organizations accounted loss of over $234,244(Whitman and Mattord, 2012).

However, a common network security problem most organizations are facing sometimes is the companies' employees and their various errors they commit. According to Whitman and Mattord (2012), Human makes mistakes are attributed to inexperience or lack of proper training and results from false assumption.

Several methods have been proposed in order to combat this. Perhaps the most popular of this is the simplest: installation of antivirus on computers or nodes. Others have proposed stronger antivirus and firewalls as a way to mitigate malicious attacks to computers. With the advent of smart devices and the advancement in technology, our computer systems, network systems and relevant information are prone and vulnerable to viruses and hackers and sometimes curious snoopers. Action is needed if we want to achieve confidentiality, integrity and availability of data and services over the network to enable the businesses work with comfort.

### 1.3 Problem Statement

The issue of complex networks and the need to maximize security within organizations network has overtime degraded the performances of networks causing the networks to slow in activities and uninteresting to use. These tremendous issues have driven network managers and administrators to manage the different types of traffic that traverse the network. Measuring

network performance has always been a complicated and indistinctive task for network engineers and administrators due to the fact that most engineers and administrators are uncertain on the methodologies that conform to their Local or Wide Area Networks.

They however, employed a general and a very simple method to test performance of their networks. This was done by sending a simple file from one system usually workstation to another usually server. Engineers often contemplated on the use of this file transfer approach which sometimes resulted in debates among them.

Most of them argued that, whenever files are being transferred over the network**,** it is not only the transfer speed that is measured but also the latency on both ends of the hard disk of the stream is taken. They also emphasized that; it is very possible for the destination system to receive more transmission rate than the source is able to send, or vice versa.

These inconsistencies generated by queuing mechanisms, operating systems hard disks and other hardware devices created unnecessary delays eventually yielding inaccurate result. They however stressed that the utmost approach for measuring the maximum throughput and related attribute of a network is to minimize the delay generated by the machines partaking the experiment. High or mid-range machines such as personal computers, servers and workstations are used to carry out the experiment. They are effectively used on the assumption that they are not sharing resources with other task during the experiment.

Despite the fact that larger companies possess the financial resources to conquer all principal challenges and procure expensive tools dedicated to scanning and analyzing network environments, the rest can depend on other techniques and equipment, which are mostly available and free from the open source environment(Wang, 2015).

## 1.4 Main Objectives

The main objectives of this research are to measure network performance to ascertain what actually happens when data traverses a network.

Moreover, the research is done to visualize the network topology thereby identifying weaker systems in networks. The ability to view the entire network at a glance, irrespective of hierarchical, physical, or geographical view, enhances rapid visibility to troubleshoot and creates rooms for upgrading.

As utilization of network increases, there is the need for a strategy to accommodate additional devices and increase bandwidth to gain competitive advantage stay ahead of demand. The research enlightens organizations to incorporate sophisticated system to be able to detect when performance degrade and react to sustain satisfactory service.

Another interesting aim is utilization of tracking trend. By means of Charting trends the significant performance of an application or the network would be well understood. Basic reports are analyzed to help pinpoint irregularities and make possibilities to take counteractive measures.

Lastly, creating a more convenient room for troubleshooting can never be overlooked in this research. The use of logical diagrams depicts distinct view for checking individual devices. Vital performance data such as availability, packet loss, response time, Ethernet delay help to diagnose problems on your network.

## 1.5 Specific Objectives

1. To identify methods to boost the performance of networks
2. To identify applications which usually congest network.

3. To restrict the network to intrusions and applications that will cause congestion on the network and ensure free flow of information.
4. To measure and ascertain the performance of applications on the network with or without protection.

### 1.6 Justification of Thesis

This thesis considers the adequacy of existing theories of implementation of complexity and Network security policies. The purpose is essentially to manage the amount of data that traverses a private or shared network through firewall technology. It also detects the network service that is likely to cause congestion on the network. There are a number of potential pitfalls that may arise if network performance is not measured properly. The thesis admonishes organizations to know the performance of their network in order to gain an edge over competitors.

Again, it enforces the protection of valuable product such as data for individual and enterprises from malicious attacks. Data destruction can affect the concerned victim profoundly. However, breaking into a system may be detectable without any difficulty, as some hackers tend to leave indications of their deeds.

The thesis argues that HTTP application generates lots of traffic on the network and degrades the performance of the network.

The thesis accordingly presents the measurement of the performances of various applications on a secured and non-secured network. The goal of this research is to understand the essence of securing complex networks and also the underlying problem they face. Emphasis was placed on studying solution on a company's Local Area Network (LAN) incorporating no, partial or all traffic to traverse the network.

## 1.7 Organization of Thesis

The thesis is organized as follows:

1. Chapter 1 presents the introduction to network security the background study to securing networks and the main and specific objectives and the justification of the study.
2. Chapter 2 describes the literature review. A detailed study is conducted on all open-standard security architecture and also discusses the flaws within them. Also some factors that influence network performances are also highlighted. The knowledge acquired from this study provides support to facilitate the buildup of the thesis.
3. Chapter 3 is a buildup of three simulation procedures which are configured with or without firewall security to improve upon the network security of an organization.
4. Chapter 4 analyses the results of the simulations when implemented to secured and complex networks. The chapter describes the performances so far as the applications are concerned.
5. Chapter 5 summarizes the findings and of the research and also discusses possible extensions that can be done.

# CHAPTER TWO

# LITERATURE REVIEW

## 2.1 Introduction

The realization for secured networks is a more or less a new requirement. Earlier in time most computers were not networked (Canavan, 2001). This was not as a result of inability to connect the computers but rather deficiency in technology. The systems were mostly mainframes or midrange that were controlled and administered centrally. Users communicated with the mainframe via dumb terminals. The capabilities of dumb terminals were limited. Terminals usually needed to be connected to a directly to a dedicated port. These ports were mostly serial connections that made use of RS-232 protocols. It normally required that, one port be used for one terminal. IBM, Digital Equipment, and other computer manufacturers developed variations on this architecture by utilizing terminal servers, but the main concept remained unchanged. According to Canavan (2001), nothing was comparable to the occurrences today where more than thousands of connections can reach a system on a single network circuit. In the 1980s, the integration of Personal Computers (PC), the development of network protocol standards, the reduction in the cost of hardware, and the development of new applications caused many people to acknowledge networking. Consequently, LANs, WANs and computing experienced tremendous growth.

Initially, LANs were relatively secured simply because they were isolated physically. They were not connected to Wide Area Networks (WANs). This standalone feature protected the network and its resources.

WANs in fact paved way for LANs and are still growing, but they were usually controlled centrally and available to only few individuals in organizations. WANs that made use of

dedicated privately owned or leased circuits were relatively secured because there were limitations to accessing the circuits (Canavan, 2001).

## 2.2 History of the Internet

According to Avolio (1999), networks and internet was not available in the early days. There was no e-mail; hence the only available means of communication was through postal mail or the telephone. However telegram was busily used by people also to reach out to others in different areas and places Of course, the introduction of the Internet has changed the manual and traditional means of communication into secured easy and more reliable means which is adapted by people. The Internet started as Advanced Research Projects Agency Network (ARPANET) and covered a small community.

Peter Yee a researcher at NASA Ames Research Center in November 2, 1988, reported an incident that occurred and change the state of the internet till date. He reported this incident, by sending a message to the TCP/IP mailing list which states "We are currently under attack from an Internet virus! It has hit Berkeley, UC San Diego, Lawrence Livermore, Stanford, and NASA Ames". The report was documented and was subsequently called "The Morris Worm" (Avolio, 1999). Researchers, contributors to the buildup of the Internet, organizations as well as other stakeholder that had commenced the usage, acknowledged at that instance that the Internet was not a platform of trusted associates. In fact, it had not been for a considerable length of time, not even years. To their advantage of the Internet community, they did not over react to the circumstance. They however, started sharing information on their practices to avert future interruptions.

The awareness about systems and network security is increasing alongside the driving force. This awareness, most likely, is generated as a result of continuous growth of the Internet and the rise in the number of organizations channeling their data and information onto the Internet. Businesses have also grown in the usage of networked computers especially sending information with e-mails and this has also driven the interest. Reports of security violations in prestigious companies in the evening news are normally presented to numerous individuals, which give indications of some robust defense that had failed to prevent some attacks. A probable outcome of these influences is that a lot of people perceive that Internet security and Internet firewalls are the same. However, most companies still place all their network security under one firewall technique knowing very well that no single mechanism provides the entire computer and network security needs of an organization, (Avolio, 1999).

In employing security certain part of the network must be fine tune to meet the desire standard of the needed quality of service. The critical component in managing data transfer is by network optimization.

Information technology has grown exponentially with more applications consuming the greater amount of bandwidth as well as producing larger volumes of data from application of which majority of these data has to flow through corporate network.

The situation is however difficult to change or improve as the rate of usage of computers keeps increasing day in and out. The only plausible solution is to improve the information technology platform and the management of data flow within the organization.

### 2.3 Factors affecting network performance

The performance of a network helps to improve and assures the quality of service the operator is providing whiles also guaranteeing optimum network utilization. Computer networks are becoming complex and maintaining security across such network in multivendor environment is becoming a big challenge. Integration of differentiated services has a great impact on the network source. Operators are also optimizing the network to improve the service quality and meet customers' needs. Some parametric models that must be studied are:

- Congestion
- Threshold
- Delay and latency
- Network utilization
- Throughput
- Jitter

#### 2.3.1 Congestion

Congestion occurs when the loads on the network is very high. It indicates clearly that the network or network devices have reached or are reaching their capacity. Generally whenever a network is congested, it results in rapid increase in delay and eventually leads to loss of data and information if the instance is not rectified. A key indication of congestion issues is Queuing delays.

#### 2.3.2 Threshold

Threshold is a value set to notify the network management system that utilization, latency or congestion is exceeding its critical limits. Managers in network management areas measure the precise behavior of networks and links. They also set up the threshold.

### 2.3.3 Throughput

Throughput is the measure of the amount of data that can be transferred from one computer to another in a specified time frame (El Gamal et al. 2004). It is used to evaluate the performance of Random Access Memory (RAM), Hard Disk and other Internet and network connections.

For instance, a Hard Disk with transfer rate of 128 Mbps has four times the throughput of a Hard Disk that can transfer data at 32 Mbps. Importantly, a 64 Mbps wireless connection has approximately eight times the throughput of an 8 Mbps connection. However, additional factors like internet connection speed and other network traffic may attribute causing limitations of the actual data transfer speed. Hence, it is advisable to understand that the maximum throughput of every computing device or network circuit may be substantially higher than the actual throughput accomplished in daily use.

### 2.3.4 Bandwidth

Bandwidth describes the rate at which data is transferred from an internet service such as a website to another computer device in a specified time or period. Therefore the efficiency and speed of the internet activity is determined by the amount of bandwidth required by that internet service. Such internet services could be opening web pages, accessing databases, downloading and uploading files and many more. In general bandwidth is measured in ‘bits per second' and sometimes ‘bytes per second'.

### 2.3.5 Delay

Delay and latency are very similar in characteristics and refers to the amount of time taken by a bit to be transmitted from one device to another device on a particular network. In short, latency is the measurement of delay from one end of a network. When the latency is high, there is an indication of long delays. In a network, especially complex networks, Latency is inevitable. It is

therefore used to measure the performance of the network. Latency or delay is subject to change based on the amount of load on the network may vary based on loads (El Gamal et al. 2004).

### 2.3.6 Jitter

It is also a function that plays the behavior of delay but varies with time. It is the random variation in the timing of data packets when the round trip of Ethernet network is affected. Jitter is caused by congestion in the network or physical link that goes down and needs to be re-established (Hancock,2004).

### 2.3.7 Network Utilization

Network utilization measures the amount of the total network resources that is used at a point in time. The ratio of current traffic to maximum traffic that Central Processing Unit (CPU) can handle is however represented by the utilization. It also measures the bandwidth consumed on the network. Whenever the utilization is high there is a clear indication that the network would be busy. On the flip side, when the utilization is very low then the indication is that the network is idle or less busy. Like latency or delay, Utilization changes with respect to the actual traffic load and the time from which it is averaged. Utilization also measures the amount of CPU loads in clients and servers (Castelli, 2002).

## 2.4 Security products affect network performance

Organizations and individuals need education on how to choose an applicable security technologies, tools, and methodologies to prevent and mitigate any security threats before they impact the business. Some widely used security products technologies in Ghana are discussed in this section. These technologies include:

a. Firewall technology

b. Virtual private networks (VPN) technology

c. Intrusion detection systems (IDS) and intrusion prevention systems (IPS)

d. Anomaly detection systems

### 2.4.1 Firewall technology

Hitherto, firewalls have been utilized as barricades to prevent intrusion and destructive forces from any given network. Currently, firewalls and security applications have many strong and sophisticated features ahead of the traditional access control rules and policies (Santos, 2007). Most available network firewall technologies offer users, organizations and application policy enforcement (that provide multi-vector attack protection) as well as other stakeholders with various types of security threats. Logging capabilities that permit network security administrators to identify, investigate, validate, and mitigate such threats are mostly provided by these firewalls. In addition, many programming applications can run on systems to ensure that only the host is protected. Applications of such nature are often referred to as personal firewalls. The overview of networks, personal firewalls and their related technologies are discussed in this section. Firewalls are used everywhere even in housing by separating a living room from a kitchen or an apartment from another. Firewalls act as barricades to fire. They are responsible for mitigating the fire until the Fire Service quenches it. Firewalls are also embedded in vehicles, separating passengers and engine compartments.

Cheswick et al. (2003) defined Internet firewalls based on the following properties:

i. As a single entry point for the passage of all traffic between two or more networks;

ii. As a traffic controller and authenticator for all traffic logged through the devices (Avolio, 1999).

Later in the 1980s, the first network firewall evolved. During those times Routers were used to separate a network into smaller Local Area Network (LANs). Firewalls were installed to mitigate the issues of one LAN overflowing and affecting the entire network. These were established to enable and assist the English Department employ any applications to its own network, and administer its network in the capacity required by the department. To avoid spillage of issues such as errors in network management, or noisy applications to trouble the whole campus network, the department was put behind a router.

The first security firewall was introduced in the early 1990s. They were Internet Protocol (IP) routers with filtering rules. These firewalls were very operative, but with some limitations. It was not easy to get the filtering rules right. Especially, it was problematic in identifying all the components of an application that may need restrictions in some cases. Meanwhile, in other cases, people navigated around. Hence, the rules needed amendment (Avolio, 1999).

Subsequently security firewalls that evolved were expounded and more adaptable. They were built on a defensive structure often called bastion hosts. Presumably, Digital Equipment Corporation (DEC) is noted to develop the first commercial firewall of the type, which used filters and application gateways such as proxies and was based on the DEC corporate firewall. Brian Reid and the engineering team at DEC's Network Systems Lab in Palo Alto originally invented The DEC firewall. Large East Coast-based chemical company, on June 13, 1991 purchased a configured the first firewall which till date is regarded as first ever commercial firewall (Avolio, 1999).

After some few months, Marcus Ranum also at DEC invented security proxies(Avolio, 1996). He reprogramed most of the remaining firewall codes. His product was created and named DEC

SEAL indicating Secure External Access Link. The DEC SEAL comprised of an external system, known as Gatekeeper, the only system the Internet could communicate with, a filtering gateway, also known as Gate, and an internal Mailhub (Avolio, 1999).

Simultaneously, Cheswick et al. (2003) had been experimenting with circuit relay-based firewalls at Bells' laboratory. They discovered and developed a firewall security called Raptor Eagle six months after DEC SEAL was introduced. They then developed ANS InterLock which followed Raptor Eagle.

Today, these firewalls have grown into profoundly high-tech tools that screens and prevent potential malicious traffic from affecting systems and networks. Firewalls currently assume the responsibility of checking requests and imposing restrictions on data at multiple levels which includes the web application level.

Possible drawbacks of Firewalls technology is that, firewalls are repulsive at detecting the idea behind people's minds and also failed at detecting data packets that can damage the system. They sometimes cannot protect attacks from insider who might log on to the network even if the insider uses a public or share network in the attack. Firewalls also cannot protect connections that do not pass through the firewall. Firewalls are noted to provide minimal protection especially with mysterious attacks, and normally provide weak protection against computer viruses and worm.

### 2.4.2 Virtual Private Network (VPN) technology

Access to Virtual Private Network (VPN) has been somewhat new concept to most organizations some years ago. While large corporations were already benefiting from the use of VPN technologies, the others were beginning to gain consciousness, realizing the potential and

possibilities VPN connections. Merchants such as Cisco, Checkpoint and Microsoft started with the production of different types of products that would provide VPN access to organizations. Currently, VPN is regarded as a standard tool when dealing with critical security and router related issues. VPN technology highly recommended among most institutions and companies worldwide (Scott et al. 1999).

A virtual private network is a way to simulate a private network over a public network, such as the Internet. It is called "virtual" because it depends on the use of virtual connections that is, temporary connections that have no real physical presence, but consist of packets routed over various machines on the Internet on an ad hoc basis. Secure virtual connections are created between two machines, a machine and a network, or two networks (Scott et al. 1999).

With VPN, virtual connections are churned out between geographically dispersed users and networks over an unrestricted network such as the Internet instead of using a dedicated connection, like telephone lines. Data is communicated as though it travelled via private connections (Lewis, 2006).

Tunneling is the means through which VPN transmits data. Packets are encapsulated or packaged differently with new header transmission. The header makes available routing information which makes it possible for data packets to move across a shared, public or untrusted network, before it reaches the endpoint of the tunnel. The encapsulated packets traverse on a logical path known as tunnel. Packets are however, “de-capsulated” and forwarded to their final destination when each data packet reaches the tunnel endpoint. Moreover, the endpoints for the two tunnels are required to support a common tunneling protocol. Tunneling protocols are normally activated and work at the OSI (Open System Interconnection) data link layer, or network layer. Some of the widely

used tunneling protocols include IPsec, L2TP, PPTP and SSL. A packet with a private non-routable IP address can be sent inside a packet with universally unique IP address, by means of extending the private network over the Internet. VPNs are modeled to replace and avoid the high cost of using needless leased lines (Lewis, 2006). Some protocols used to implement VPN are:

i. Point-to-Point Tunneling Protocol (PPTP)
ii. Layer 2 Forwarding (L2F) Protocol
iii. Layer 2 Tunneling Protocol (L2TP)
iv. Generic Routing Encapsulation (GRE) Protocol
v. Multiprotocol Label Switching (MPLS) VPN
vi. Internet Protocol Security (IPsec)
vii. Secure Socket Layer (SSL)

VPN implementations can be categorized into two distinct groups:

i. Site to site VPNs: With this implementation companies and organizations are permitted to set up VPN tunnels between two or more sites to effect communication among them over a public network. Numerous organizations utilize IPsec, GRE and MPLS to build site to site VPN protocols.
ii. Remote Access VPNs: This permits users to access the organization's network from remote locations such as their homes, hotels, conference halls and any other place as though they were connected to their company's network directly.

One particular reason why company's use VPN technology is that, its encryption capabilities provides data confidentiality. Once a connection is established, the VPN utilizes some of the tunneling mechanisms stated above to encapsulate encrypted data into a secure tunnel, with plain

read headers that can travel on a shared network. Without proper decryption keys, data packets which traverse a public network are unreadable. Thus data packet is not unveiled or altered in any way during the course of transmission. In addition, VPN technology provides checks on the integrity of data. This is usually performed by using a message digest to make sure and verify that the data has not been manipulated throughout the transmission.

VPN technology does actually not grant or enforce strong user authentication. Users however simply type username and password to gain access to a company's internal private network from a remote location via other insecure and untrusted public network such as the internet. Nevertheless, VPN does support supplementary authentication methods, such as smart cards tokens and RADIUS.

### 2.4.3 Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Intrusion Detection Systems (IDSs) are devices that in an unrestricted mode detects efforts that a hacker made to gain unauthorized access to a network or a host to degrade its performance or to steal vital information (Santos, 2007). They are also security systems that act as a protection layer to the infrastructure (Mohammed et al. 2012). They detect distributed denial of service (DDoS) attacks, worms, and virus outbreaks. Additionally, Intrusion Prevention Systems (IPS) are devices which are capable of sensing all these threats; however, they are also capable of dropping non-compliant packets inline. Packets that do not conform to security policies are not allowed through the protected network. This is the major difference between IDS and IPS systems.

The concept of monitoring user activity through logs and computer records was first introduced by Jim Anderson (Mohammed et al. 2012). This was preconceived to protect information from

unauthorized access by both external and internal users and also to protect information from people who intend misuse their privilege. This was the initial intent behind the introduction of host based IDS. Ever since, the concept has been researched and improved to meet the requirement of the growing public usage of internet with its shared weaknesses. The first real time intrusion detection system is called Intrusion Detection Expert System (IDES): Researchers at the Computer Science Laboratory at SRI International conducted the research on IDES. IDES stands out to be an independent real-time intrusion detection system that integrates the concept of anomaly and rule based detection. Anomaly based detection used statistical algorithm while expert system was used to create the ruled based components. It is known to be an independent system since it is not bonded to any specific system, environment, vulnerability or any form of intrusion. The IDES model was unveiled in 1886 to serve a general purpose and its framework was to be used as basics for developing variety of sophisticated and powerful IDS. IDS technology is now widespread in well research field because of its high demand in the industry. The persistent interest in this technology by users and organizations has continuously improved IDS performance and accuracy.

Since the formation of IDES there are many more intrusion detection products in the market for users to choose and implement. According to Mohammed et al. (2012), Kevin Richards reviewed the five different IDS products to measure their performances in the production environment. In his review, he elaborated and emphasized on the importance of the packet processing engine in IDS. He however, stressed that if the engine is not effective and efficient the IDS sensor will begin to decline and this will reduce the capabilities of detecting attacks especially attacks involving multiple packets which need to be assembled.

### 2.4.4 Anomaly Detection System

IDS and IPS provide excellent protection against application layer attacks. However, they have vulnerability thus they are repulsive at detecting Distributed Denial of Service (DDoS) attacks which carries valid packets. IDS and IPS devices are optimized for signature-based application layer attack detection. Anyway most of them do not support day-zero protection.

Anomaly-based detection systems are very good at mitigating DDoS attacks and day-zero eruptions. Usually, the job of Anomaly Detection System is to monitors network traffic and signal or reacts to any rapid increment in traffic and any other irregularities. Based on the theories of detection, diversion, verification, and forwarding Cisco developed an extensive DDoS solution to help maintain full protection. Some sophisticated anomaly detection systems that were developed are the Cisco Traffic Anomaly Detectors and the Cisco Guard DDoS Mitigation Appliances.

## 2.5 Attacks on Network Security

An attack is an act of taking advantage of vulnerabilities to compromise a controlled system. Threat agents capitalize on these vulnerabilities to damages or steals organization's information or physical asset through attacks. Vulnerability is identified as weakness in a controlled system, where control mechanisms are obsolete and no longer effective. Unlike threats, which are always available, attacks only exist when that specific act may cause loss of information. For example, the threat of damage from a thunderstorm is present throughout the summer in many places, but an attack and its associated risk of loss only exist for the duration of an actual thunderstorm (Whitman and Mattord, 2012).

Computer devices are designed to execute instruction in a stepwise manner. These instructions in most cases are for useful purposes such as calculating values, maintaining databases and communicating with users and other systems. Sometimes, however, the instructions executed can be harmful or malicious naturally. When the damage occurred by accident, it means the code had a software bug.

Perhaps unexpected program behavior is commonly cause by bugs. In the case where the source of the damaged instructions is caused by a programmer, such instructions are referred to as malicious code or a programmed threat. Malicious software is also termed as malware. Several kinds of programmed threats are available for destruction of information.

Computer scientists have categorized threats according to the way they behave, the way they are initiated and the manner in which they disseminate. Recently, the media and other individual have been describing eruptions of these programmed threats generally as viruses. However, the presence of viruses in malicious codes is just a small portion of the code that has been written. Hence to say that all data losses are caused by viruses is inaccurate as saying all human diseases are caused by viruses.

**2.6 Malicious Software**

Major malicious programs that are used to attack controlled systems are discussed in the following sections.

i. Security Tools and Kits: These tools are specially designed for security professionals to protect their websites and portals against possible threats. Unauthorized individuals however use it to probe for possible weakness.

ii. Logic Bomb: These are unseen aspects in computer programs that blow out after some specific conditions are met (Garfinkel and Spafford, 1996).

iii. Back Doors or Trap Doors: They are sets of codes written into applications and operating systems to permit programmers to gain access to programs without necessitating them to undergo the usual procedures of access authentication(Garfinkel and Spafford, 1996).

iv. Trojan Horses: Trojan horses are christened after Trojan horse of myth. Trojan Horses nowadays disguise itself as the program intended to be executed by the user like games, media players, spreadsheets and text editor. Even though the program appears to be executing the necessary task of the user, it would actually be performing something irrelevant to its publicized goal without the knowledge of user's. For instance, the user may assume the program to be a game or an editor but in reality, it may be removing files, formatting disks or sometimes be modifying information. Before the user could realize it would be too late only to see the interface of the program the user means to run. Unfortunately, Trojan horses are as regular as jokes within some programming environments. They are normally posted as cruel tricks found on bulletin boards (Garfinkel and Spafford, 1996).

## 2.7 Computer Virus

A computer virus is a series of code that is appended to other executable code so that when the regular program is executed, the viral code is executed as well (Garfinkel and Spafford, 1996). The viral code replicates itself and causes it to be appended to several other programs. Viruses cannot execute on their own. They therefore, need to have a host program, of which they form part to be executed to trigger them. In short viruses are not distinct programs.

It was not until the 1987 that computer viruses started to gain attention in the popular press and also the trade and technical press worldwide. Lately in October 1987 computer viruses struck at two universities in United States and one other in Israel. A virus known as The Brain or Pakistani virus struck at the University of Delaware in October 1987. Arguably", The Brain" is learnt to be the first real computer virus that attacked International Business Machine (IBM) computer users in the mid-1980s. Really, "The Brain" was a virus that attacked the boot sector (Highlands, 1997).

Months after the discovery of the Brain virus, a University in Pennsylvania broke through with another virus known as Lehigh or COMMAND.COM virus. Later, a virus also attacked the Hebrew University in Jerusalem. In its findings, they discovered Friday the 13th virus but also exposed the two variations of the April 1st or April fool virus in the course of the search. These cases introduced and categorized computer viruses into two different types namely the Brain and the Lehigh virus. One type affected boot sectors that are the (Brain virus) and the other type affected executable codes that (the Lehigh and Israeli virus). The Brain, also known as Pakistani virus infected boot sectors. The Lehigh and Israeli viruses infected executable code. However the Lehigh virus infected only COMMAND.COM while the Israeli viruses attached itself to the .EXE and .COM programs. The three viruses also contrasted in terms of media attack. Among them, the Lehigh virus harmed both floppy and hard disks; the other two infected only floppy disks (Highlands, 1997).

These were the initial forms of the viruses. Subsequently, a number of modifications or transformations have also evolved. Another difference was the destructions or operational problems initiated by these viruses. The Brain at times damaged numerous sectors of a disk but

sometimes has some limitations to the damage. The Lehigh virus, subject to its host, may destroy a complete disk after a considerable number of DOS activities.

The Israeli viruses could replicate and cause an increase of programs sizes. Even though majority of viruses will not damage a previously infected system, the coding some of the Israeli viruses was faulty. It allowed the reinfection of a tainted program. As a result of the viral infection most programs could not execute because of inadequate memory. In other instances, the virus maintained part of itself concealed in bad sectors while there was a considerable rise in program execution time (Highlands, 1997). Viruses are normally found on personal computers such as Apple Macintosh and the IBM PC which run unprotected operating systems. With increasing usage of web browsers and their associates, together with increasing market for cross platform compatibility of office productivity tools has led to a situation where viruses and Trojan horses can grow and disseminate.

### 2.8 Computer Worm

A Computer Worm behaves just as the computer virus. It is a computer program that replicates itself. But the slight difference is that a virus attaches itself to an executable program, and form part of it while a worm is capable of executing and propagating by itself. A worm does not attach itself to any program.

In brief, a real computer virus is comparable to an organism which depends on a host to survive. In this instance the executable program is the host. A computer worm does not depend on any host; it spreads by itself. The first computer worm was introduced by John Shoch at the renowned Xerox PARC (Palo Alto Research Center). Shoch was an engineer at PARC and was at the time studying for his Stanford doctorate when he created the worm. The worm program

was christened after the “tapeworm”, a program that surfaced in a well-known science-fiction novel of the time by John Brunner called “The Shockwave Rider”. This science-fiction novel sarcastically assisted in promoting the concept of a replicating program more than other more critical writings on the subject (Fosnock, 2005).

The next worm emerged as a joke or innocent prank. It was also part of the earlier and most significant worms to succeed as a network exploit. The worm started on the German EARN network, disseminated through connected Bitnet sites and finally moved through Bitnet connections to cause destructions on the IBM Internal File Transfer Network which was also known in United States as VNET (Fosnock, 2005). This worm was named the Christma Exec.

In spite of the introduction of two complete efficient worms, many people persisted in treating computer worms as indistinct hypothetical problem. It was until the late 1988 a college student known as Robert Morris, Sr. released the outrageous Internet Worm, which was also known as the Morris worm or the “Great worm” which changed that perception about worms on the new and unsuspicious internet. The Morris worm was a “Multi Mode” worm which damaged servers that run BSD and Sun operating systems. Weak passwords and well-known vulnerabilities in mail applications were also exploited by the Morris worm. The concept behind the Morris worm was not to cause system damage, however, bug in the software permitted the worm to infect and attack other servers countless times. Therefore, any other instance of the worm on the server resulted in the consumption of extra CPU resources. The servers operated slowly and this eventually originated the first Denial of Service attack (Fosnock, 2005). During the period of the attack, it was projected that the Morris worm had tainted nearly 6,000 servers which is approximately 10% of the Internet servers, and had instigated between $10 and $100 million loss.

Teaching of the past is that, attacks will only continue to get more advanced with time. Continuous research on network performances probably makes the future.

# CHAPTER THREE

# METHODOLOGY

## 3.1 Introduction

To measure the performance and the behavior of networks and networking device with varying security strength, simulations and analytical study are used. In this research work, the study of network performance with change in security is solely based on simulation. This Chapter deals with three scenarios which are modeled using Riverbed Academic Edition 17.5 as a simulation tool.

Vehicle Inspection and Technical Organization (VITO) has 60 computers which are connected to various servers on the cloud. Security features are configured and used to block some of the application on the network to ascertain the security performance on the network. Users at other branches of the company use various online applications which include web browsing, keeping and updating records, accessing databases as well as uploading and downloading files. In addition, it is assumed that users are viewing illegal websites and transferring illegal file, pirating music, videos and software. The mission statement of VITO is to access and inspect vehicles and issue them with road worthy certificates. The road worthy certificate is required to have a response time of five seconds. This research evaluates a three network topologies with no security, limited security and advanced security policies and the performance of the network is measured. To start, a scenario to measure the network performance with no security measures thus, when no packets are blocked. Detailed explanations of all the scenarios are discussed in the sections below.

### 3.2 Riverbed Modeler Academic Edition

Riverbed Modeler is a simulation tool for modeling and designing communication protocols and network equipment. Riverbed Modeler stands out to be one of the leading simulators for industrial and academic research to design and study the performance of networks and networked devices. The virtual environment of Riverbed Modeler enhances modeling, analyses, and prediction of the performance of IT infrastructures, which includes applications, servers, nodes, links and other networking technologies. The virtual approach saves time, cost and the energy to build the real network so as to plan and test network conditions and effect changes. Network designers use Riverbed Modeler gain well knowledge of the project the in the product development process. This reduces the amount of time spent and also decreases the cost of expensive hardware prototyping. Riverbed Modeler Academic Edition is a limited version for educational users whose desire is to use the software for network research. It provides tools for all phases of a study which includes network design, network simulation, data collection, and data analysis. Other benefits associated with the use of Riverbed Modeler include:

i. Creating a network topology

ii. Choosing statistics

iii. Running the simulation

iv. Analyzing and comparing the results

These elements are used in order to create network models with Riverbed Modeler: Project, Scenario, Objects, Applications Definition Configuration Node, Profile Definition Configuration Node, servers, routers and other networking nodes such as computers and the internet.

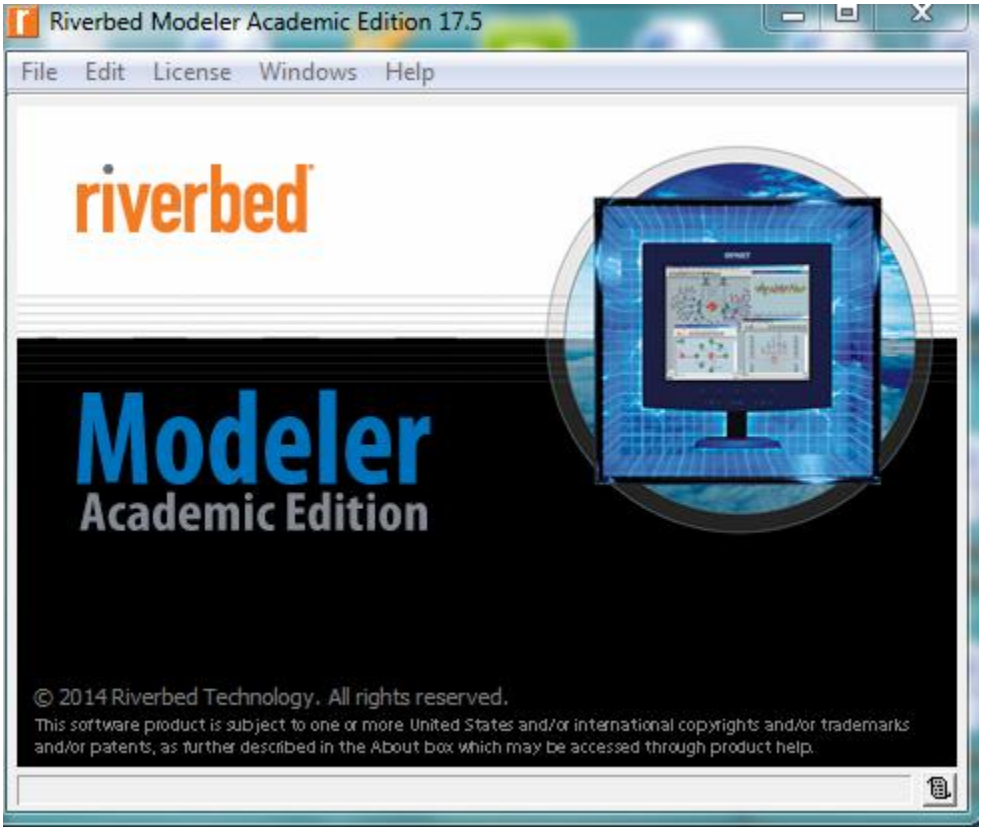



**Figure 3.1 Riverbed Startup Screen**

### 3.2.1 Project

A project in section 3.2 simply implies a network simulation. In the project the objects that will constitute the simulation, the applications that will run on the network and the different servers that will run these applications are dragged onto the workspace.

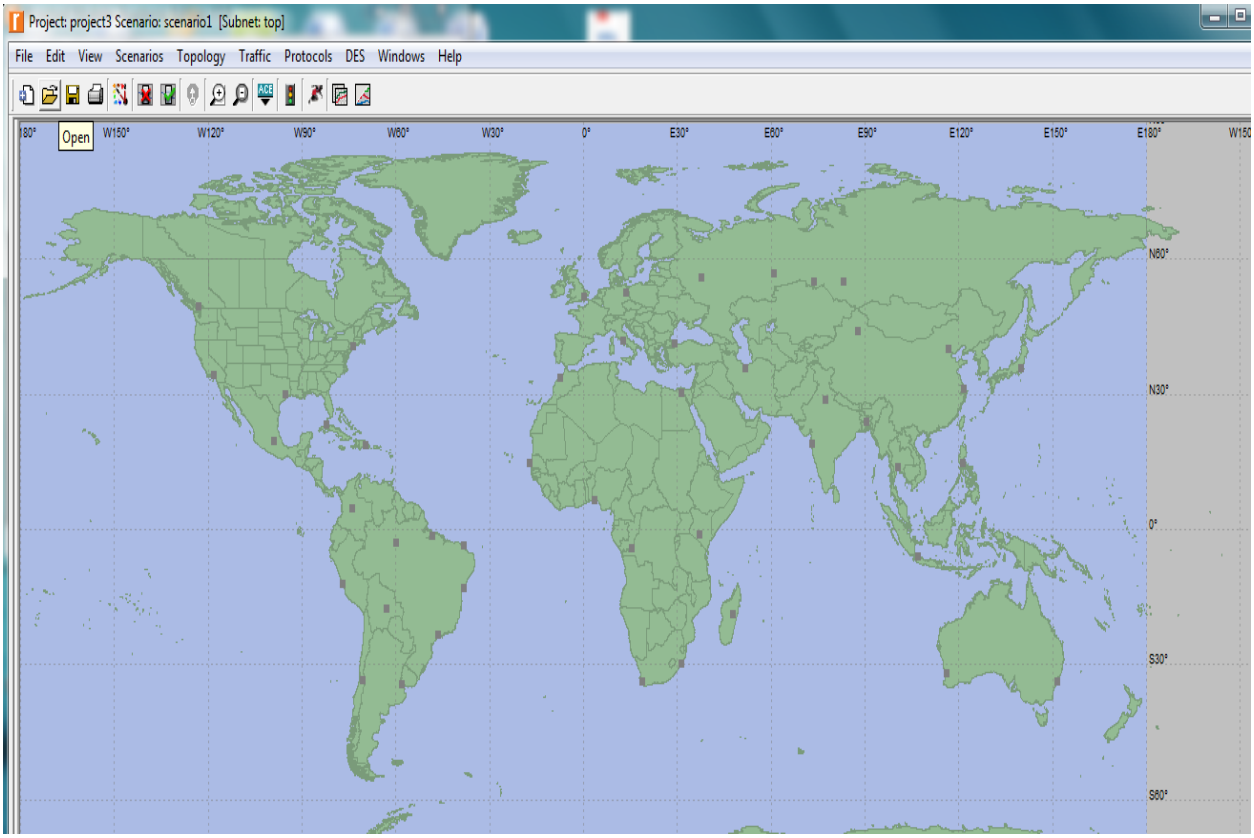



**Figure 3.2 Project**

To select devices for a project:

Select open object pallet from topology menu or click on its icon from the standard toolbar. Drag and drop the required devices for the network simulation from the object pallet box. There are two types of devices of which can be selected; these are Nodes and Links. Nodes represent devices that send and receive information. They include switch, workstation, printer, and server. Links on the other hand represent the channel through which nodes are connected to one another to establish a communication between them. Links are either electrical or fiber optic cables.

### 3.2.2 Scenario

Scenarios are used to alter a project to facilitate comparative analysis for varying conditions in order to study what if analysis. Riverbed Modeler offers the possibility to compare and analyze distinct scenarios for which these scenarios can be created and duplicated as such. Some few modifications are made to the each duplicated scenario as required by the research for the simulation. For instance, attributes of objects may be altered to ascertain how the changes affect the network performance. This consists of change in devices switching speed of the LAN or possibly altering loads traversing the network. Figure 3.2 shows a representation of a scenario.

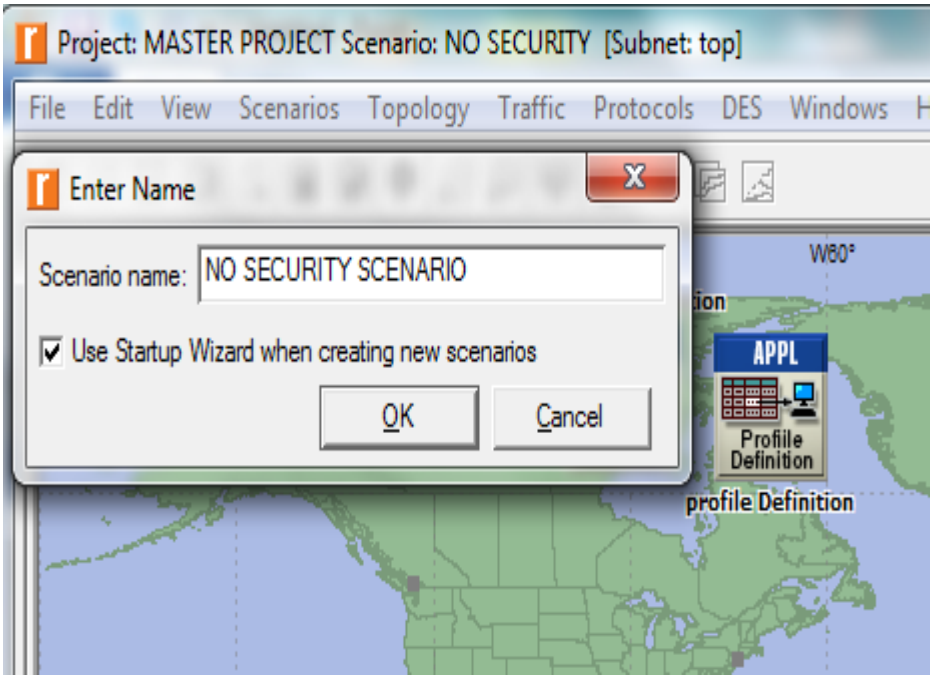



**Figure 3.3 Representation of a scenario**

In modeling a new network, it is necessary to first create a new project with two or more scenarios. A project is a collection of interrelated scenarios. Each scenario deals with separate phases of the network.

### 3.2.3 An object

An object in Riverbed Modeler is device that appears in a real network of the simulation. The object could be anything that can be dragged and dropped into a project. Examples of objects are workstations, servers, firewalls, switches, routers. Any object has attributes that define how it operates in the simulation.

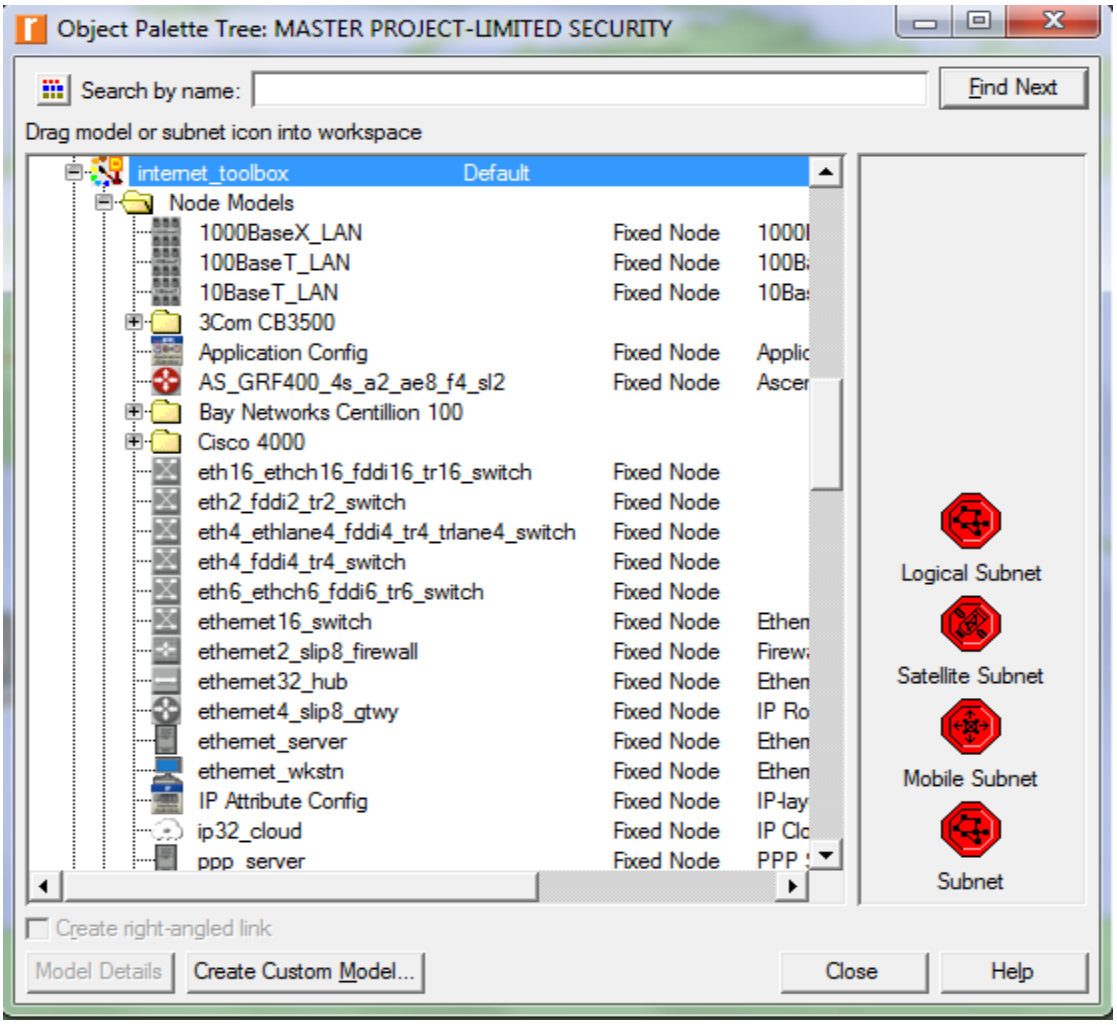



**Figure 3.4 Object palette window**

### 3.2.4 Application Definition Node

It is an exceptional element that is utilized by several projects to define the kinds of applications that will cause traffic on the network. This exceptional element is the Applications node. It comprise of the attributes for the various applications used in the network, such as Web browsing, FTP, database and so on.

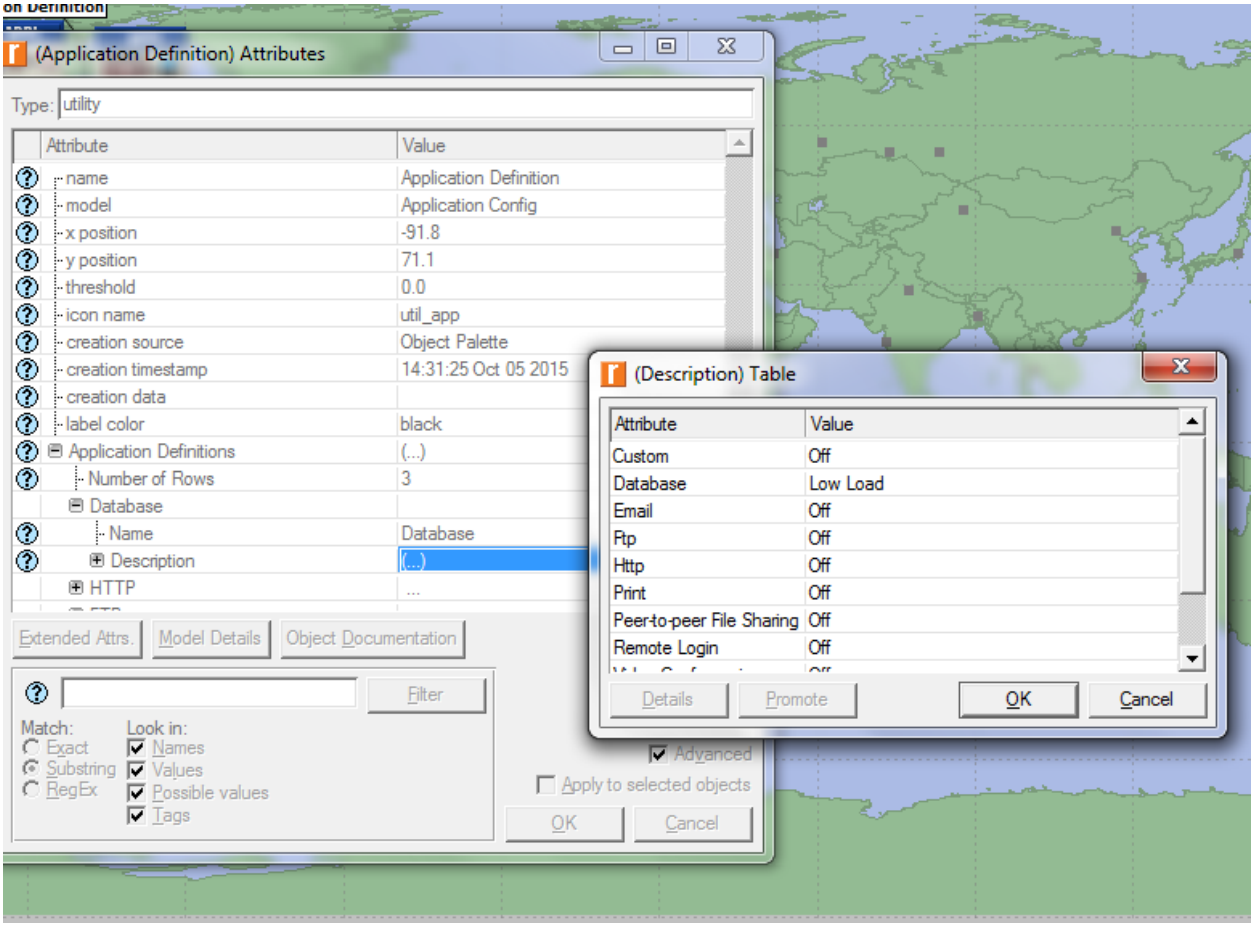



**Figure 3.5 Application definition Tables**

### 3.2.5 Profile Definition Node

The last element commonly used is the Profiles node. This object is also dragged onto the project workspace. The Profiles object is used to associate the applications with the objects that will utilize them.

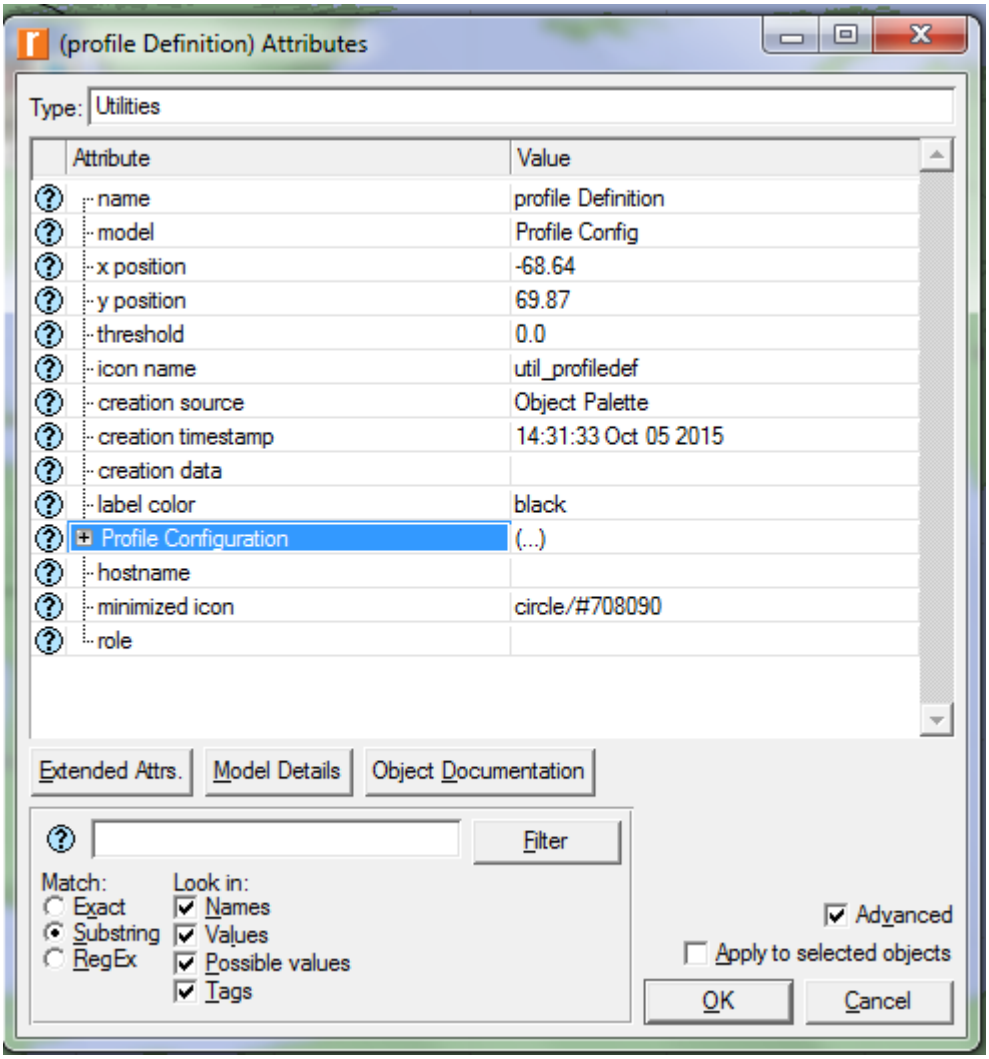



**Figure 3.6 Profile configuration Tables**

### 3.3 Network design and simulation

This section presents the actual network design and simulation of the research work. The three scenarios which include: no security scenario, limited security scenario, advanced security scenario are modeled here.

#### 3.3.1 No security Scenario

In this scenario no security is imposed on the entire network. An IP based cloud acts as the internet and connects two or more subnets being the three servers and the company's LAN. Two routers are connected across network simulation. Three different applications are set up on this scenario; these are database application, HTTP application and FTP applications. The needed traffic is generated by configuring both the Application and Profile configuration objects.

After the required configurations are done the performance of the cloud in terms of database applications, HTTP application and FTP application is evaluated. A new project is created by clicking "File" menu and selecting "New project" as in Figure 3.7

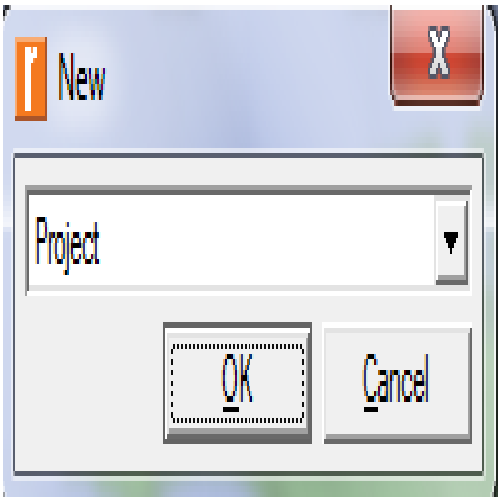



**Figure 3.7 New Project**

The internet used in this experiment incorporates 60 workstations. The simulation is done such that for No security scenario, all the 60 workstations gain access to the database application, web application and use FTP to download and upload file onto the file server.

### 3.3.2 Limited security scenarios

With limited security scenario, a firewall is installed on the network to filter packets. A duplicate of the first scenario is created with a configured firewall filtering capabilities. Here, a packet latency of 0.05 seconds is set on the network to filter packets. The same performance metrics for the No security scenario are used to measure the network performance.

### 3.3.3 Advance security scenarios

This scenario is designed by making a duplicate of the second scenario. The need for this is to filter packets and prevent illegal HTTP access. After all the scenarios are designed, the simulation is run for a period of one hour. The network performance is hence, measured.

### 3.3.4 Performance metrics

i. DB query response time

ii. DB query traffic sent and received

iii. HTTP page response time

iv. HTTP traffic received and sent is also analyzed

v. FTP download and upload response time

vi. FTP traffic sent and received is also measured

vii. Ethernet Delay

The same performance metrics is used to measure the performances of the other scenarios. Packet sizes of 10MB (low), 50MB(medium) and 100MB(high) are imposed on the network and

a switching speed of 5Mbps, 1Gbps and 5Gbps are set between the router and the cloud. The performance is evaluated for each packet size based on the performance metrics in section 3.3.4

### 3.4 Simulation Procedure

Since the goal of this research is to find the outcome of maximizing security with varying controls and measuring the performance of a network and also to evaluate the relationship between network security and performance and the effect of security for three different scenarios like No security, Limited security and Advanced security, Riverbed Modeler Academic Edition is the simulator for this experiment. The following sections explain the experiment.

#### 3.4.1 Simulation of No Security Scenario

In this section, the procedure to simulate a network with no security case is presented. Firewall is a device that imposes some limitations and restrictions on transfer of data over a network. Firewalls monitors and controls the traffic that traverses a network. Firewall of this kind is used for this experiment. In this simulation an office LAN is used as the endpoint and all transmissions are done via the cloud and firewall devices. A new project is created and project name and scenario are given as Master Project and No Security scenario as shown.

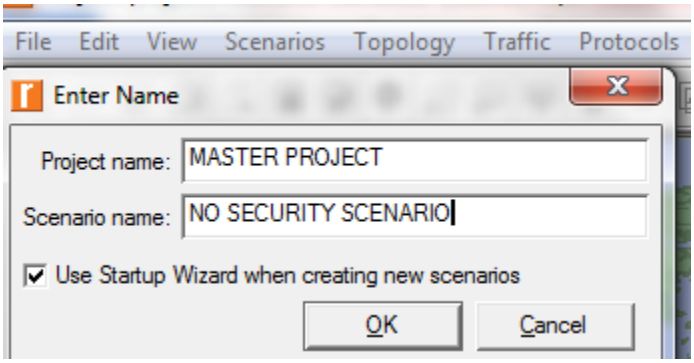



**Figure 3.8 No security scenario**

On the menu bar perform the following actions to create a basic topology

i. Click on file

ii. Click on new

iii. A new project dialog box appears

iv. Click on ok

v. In the new window, type the project name and scenario name in the project name text box and scenario text box respectively and click ok

After setting up the required project and scenario name, these steps are followed to design the simulation.

i. Select Create Empty scenario and click on next

ii. Choose The World and click next

iii. Select United States on the map

iv. Click twice on “next”

v. The workspace is then displayed

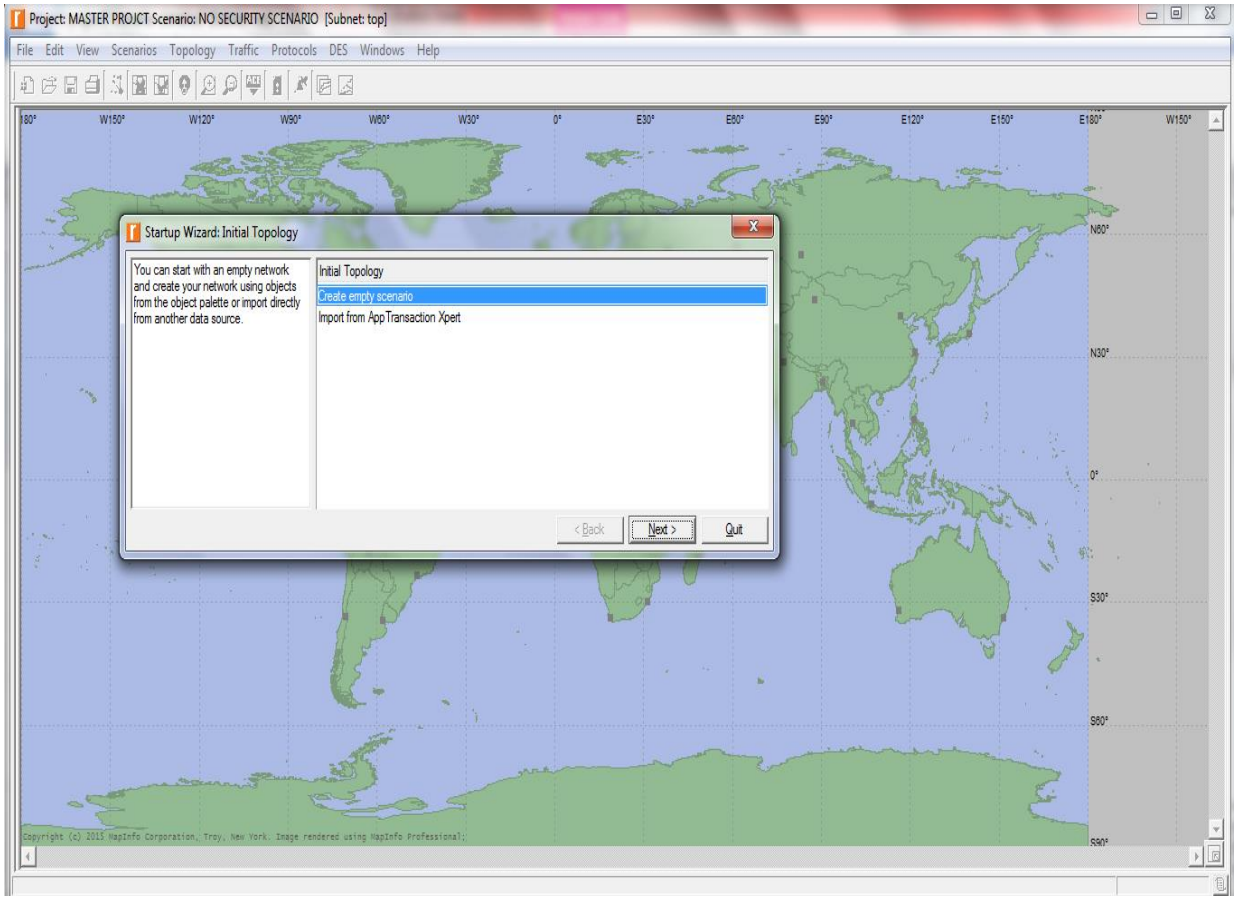



**Figure 3.9 Empty scenario**

The following objects are dragged onto the workspace:

i. The Application configuration object is used to set up the required applications. Database, FTP and HTTP applications are used on the network.

ii. The Profile configuration object is used to configure the profiles

iii. Ip32_cloud object is used to perform the function of the internet

iv. Two Ethernet4_slip8_gtwy's are used to perform the function of two routers

v. 10BaseT_LAN object is used perform the function of the office network which supports 60 workstations

vi. Three server namely database FTP and HTTP are used to support the applications

vii. Ethernet 10BaseT link is used to connect the LAN and the router

### 3.4.2 Application Configuration

Three applications are established which generate the requisite traffic over the internet or cloud. Riverbed Modeler Academic Edition makes available an object called Application Config which is used to create the needed applications on the network. The following procedures explain the configuration of the applications.

i. Right-click on Application Definition object and select Edit attributes

ii. Add three rows to the Applications definitions table, to enable the creation of three application

iii. Rename the first row as Database and select low load against the Database application

iv. Rename the other row as HTTP and select light browsing against HTTP application

v. Finally rename the last row as FTP and choose low load against FTP application

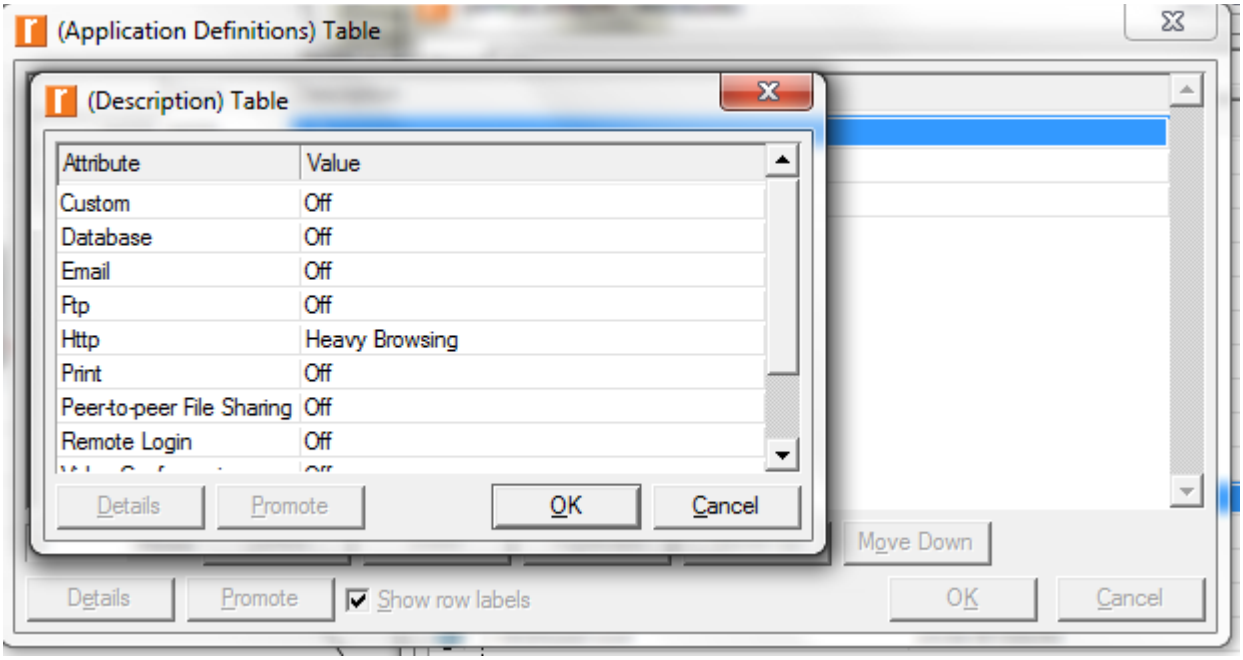



**Figure 3.10 HTTP Application Configurations**

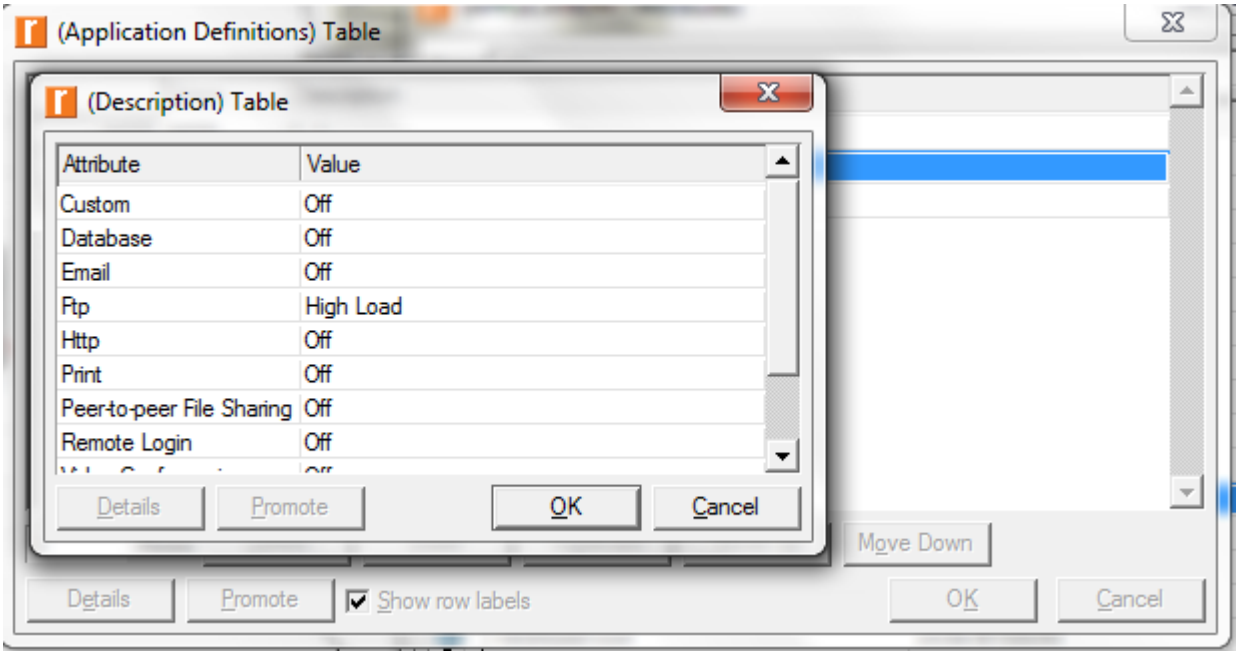



**Figure 3.11 FTP Application configurations**

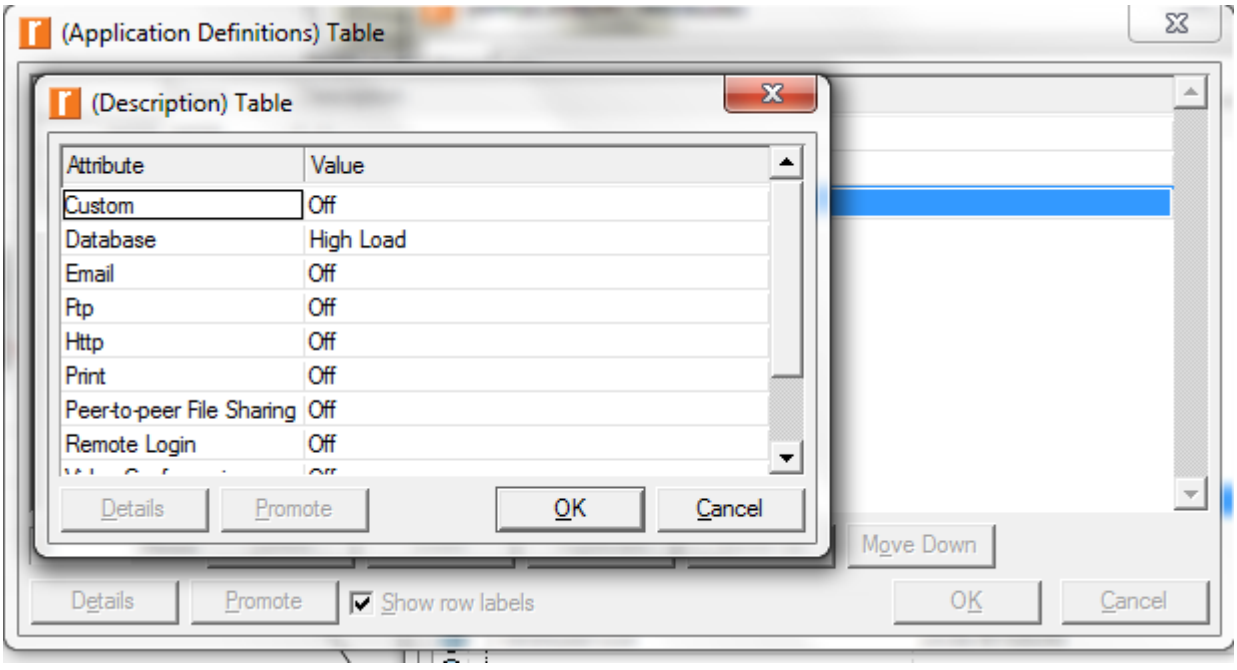



**Figure 3.12 Database Application configuration**

### 3.4.3 Profile Configuration

An application needs to generate traffic over the internet. Riverbed Modeler offers a Profile Configuration object which is used to generate the necessary traffic. The steps below detail how to configure the profile definition:

i. Right-click on Profile configuration object and choose Edit attributes

ii. Add three rows for configuration

iii. Name the first row “Accounts” and select Database as its corresponding application

iv. Name the second row as “Sales” and select FTP as its corresponding application

v. Name the last row as “Human Resource” and select HTTP as its corresponding application as shown in Figure 3.13.

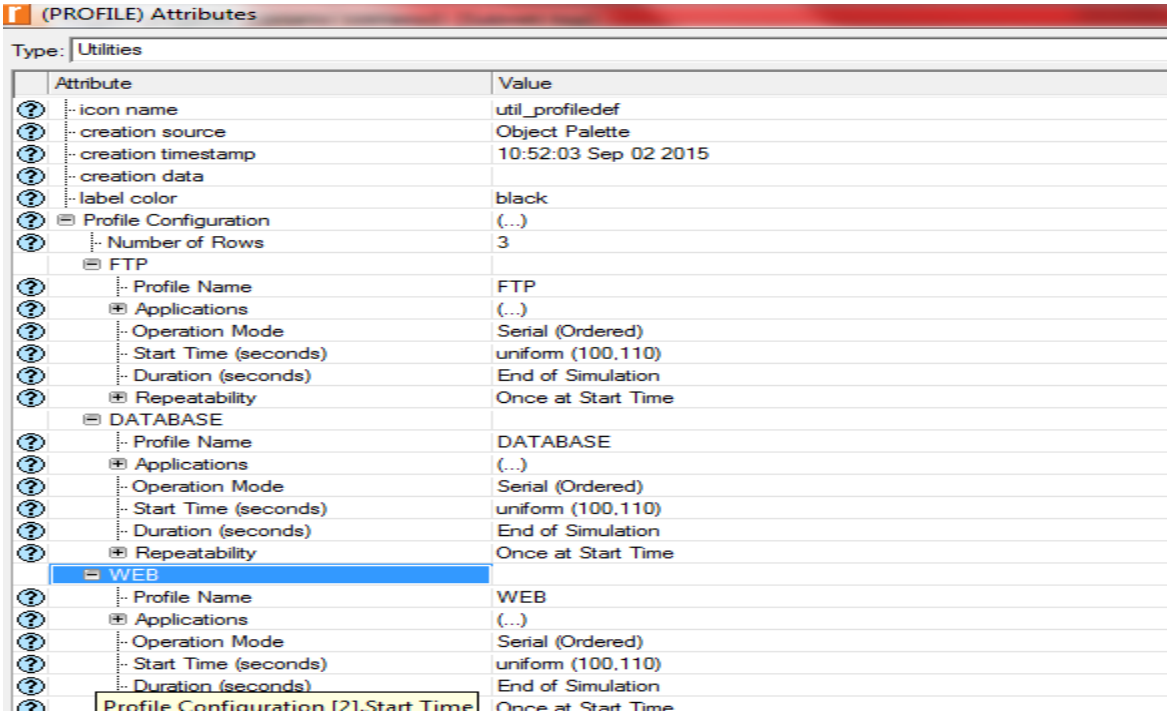



**Figure 3.13 Profile configuration**

### 3.4.4 Internet configuration

Riverbed Modeler makes available an IP32 cloud which performs the function of a simple public internet based cloud. In this research the cloud is used to support the three applications. The steps show how to configure the cloud or internet.

i. Right click on the cloud and select Edit attributes

ii. Change the Packet latency by setting its value to 0.05 seconds

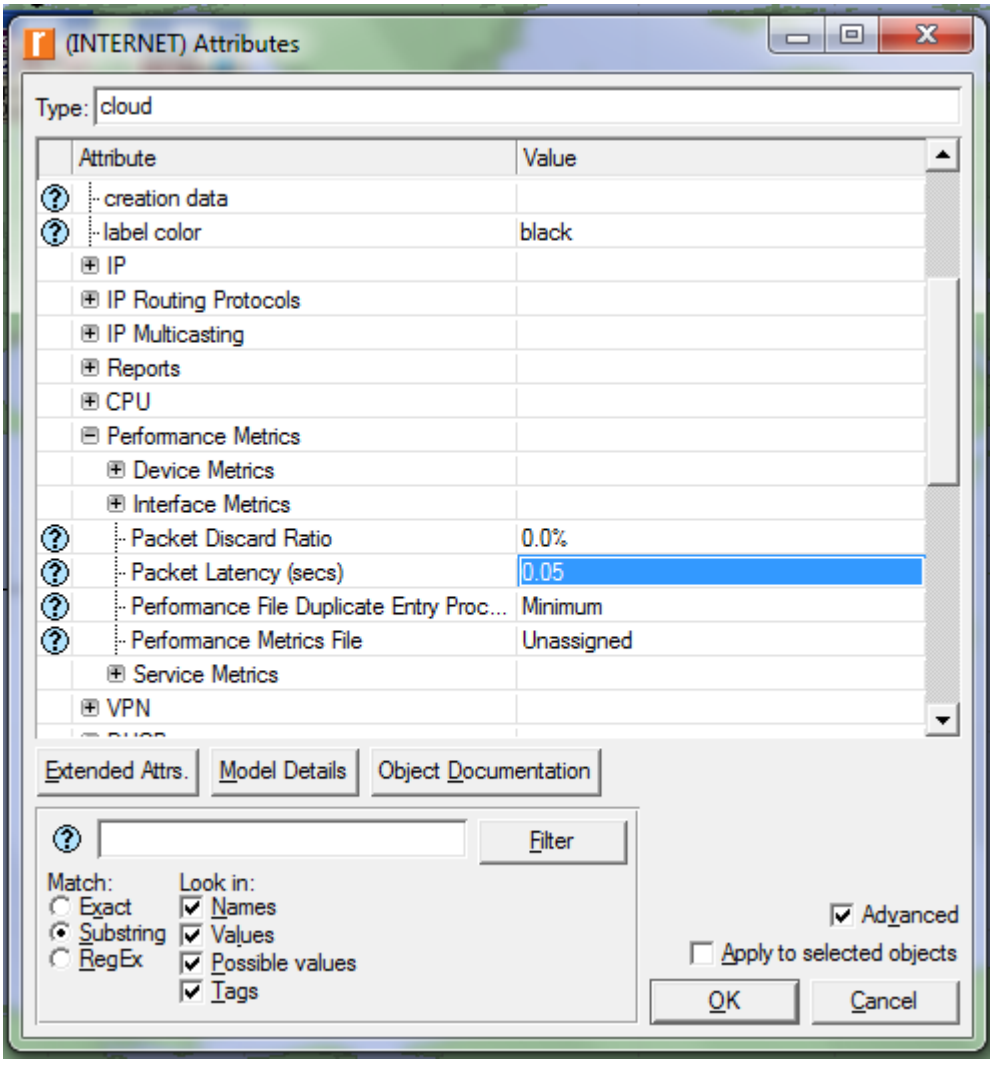



**Figure 3.14 Internet configuration**

Setting packet latency to 0.05 it implies that, the utmost packet delay across the internet as a result of HTTP, FTP and database applications is 0.05seconds. Every packet travels over the cloud with a limited delay of 0.05 seconds.

### 3.4.5 Company LAN Configuration

The company's network is built with a 10BaseT_Switch_LAN and the following steps show how the LAN is configured:

i. Right click on Company LAN and click on edit attributes

ii. Set number of workstations to 60

iii. Expand Application supported profiles and add three rows

iv. Add Database profile to the applications and set the number of users to Entire LAN

v. Add HTTP profile to the applications and set the number of user to Entire LAN as depicted by the figure below

vi. The FTP profile are also added and the number of users are each set to Entire LAN

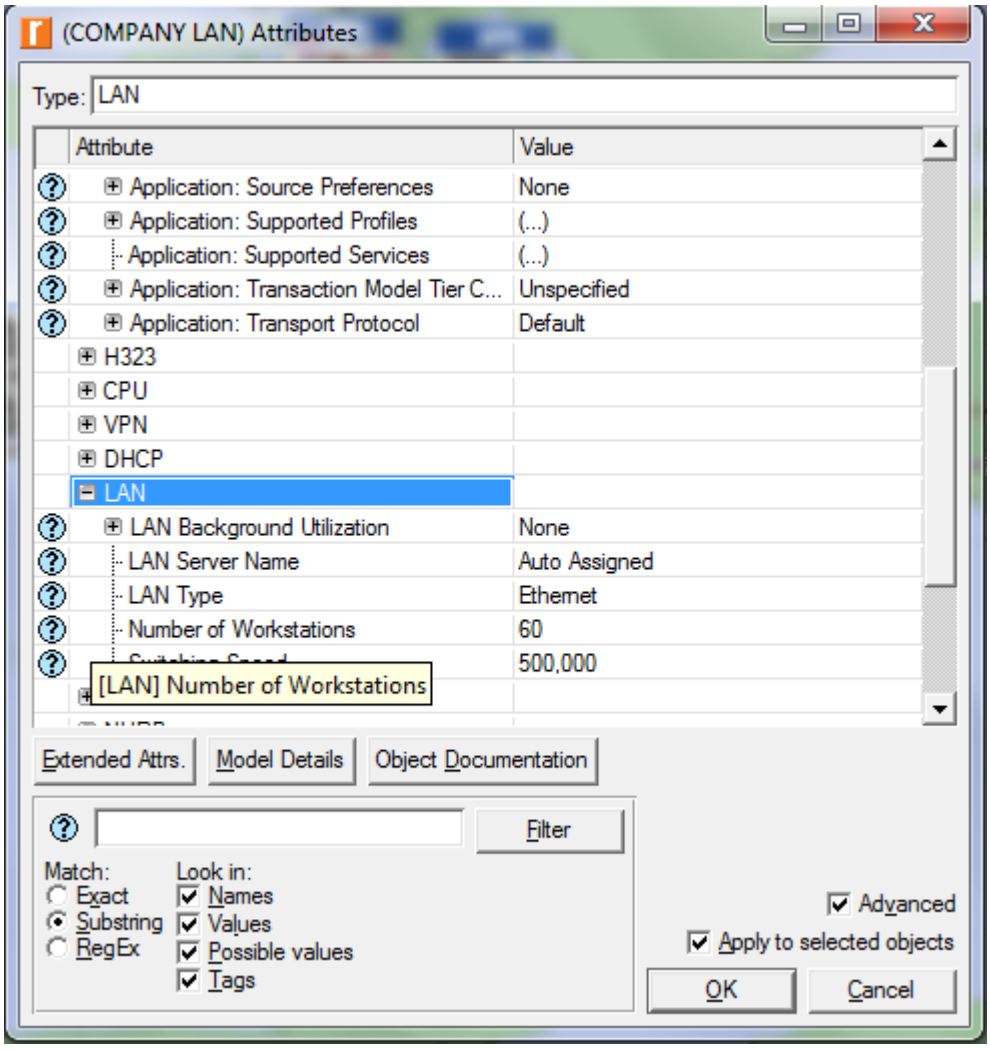



**Figure 3.15 Company LAN**

The Company's network is connected to the Router 1 using 10BaseT links which is in turn connected to Router 2

### 3.4.6 Server Configuration

Three Ethernet servers' are dragged unto the project and configured to support database, HTTP and FTP applications respectively in the following steps.

i. Right click on the database server and select edit attributes

ii. Edit the application supported profiles and set Database application as supported

iii. A similar approach is used to configure the HTTP server, where the HTTP application is set as supported

iv. Same steps are configured for the file server , where FTP application are supported

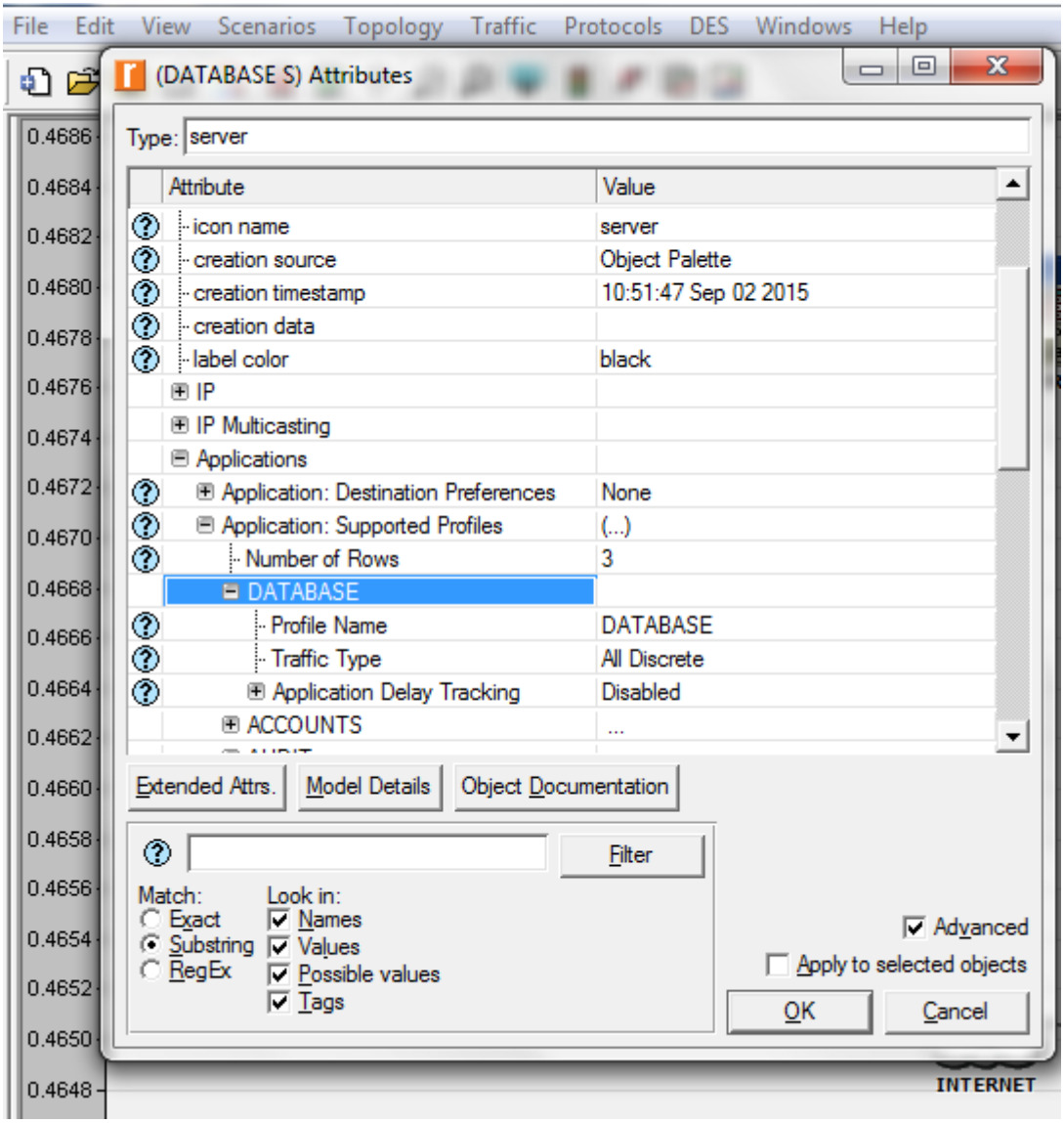



**Figure 3.16 Database server configurations**

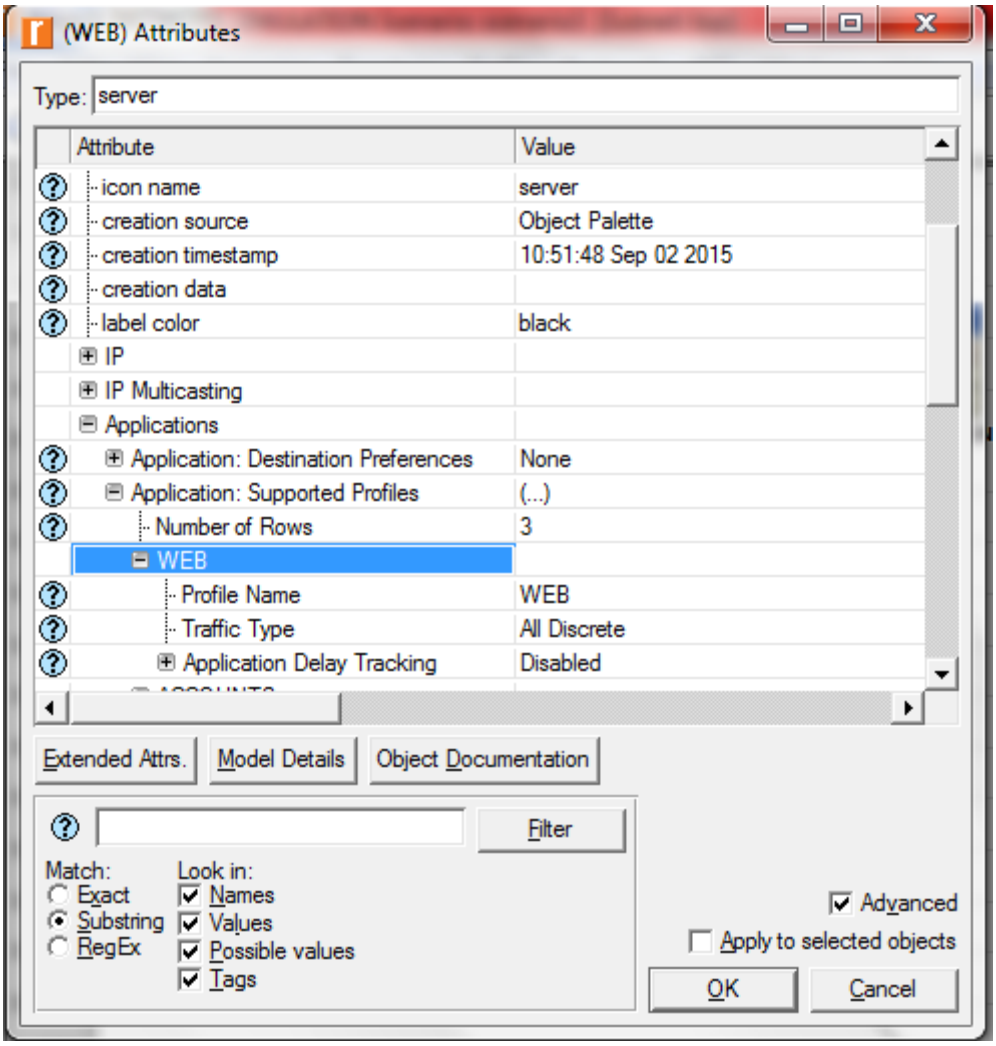



**Figure 3.17 http server configuration**

### 3.4.7 Router configuration

Router used in the simulation is the Ethernet4_slip8_gtwy object. The link between them is DS1 and T1 which are connected to IP32 cloud and the remote servers. Router 1 and router 2 were used for load balancing purposes the following step shows how it was configured.

i. Click on the Descrete Event Simulation

ii. Click on the configuring/Run DES

iii. Click on IP and expand its attributes

iv. Change the IP Dynamic Routing Protocol from default to OSPF

### 3.4.8 Performance Metrics configuration

To measure the performance of cloud against the all three applications few parameters are required. Riverbed Modeler provides three levels to measure performance of a network. These are the global level, node level and link level. In this research the Global level is used to measure the performance of applications on the network. Global level is configured as:

i. Click on DES menu and select Individual statistics

ii. A new window opens with the options to global statistics, node statistics and link level statistics shown in Figure 3.18

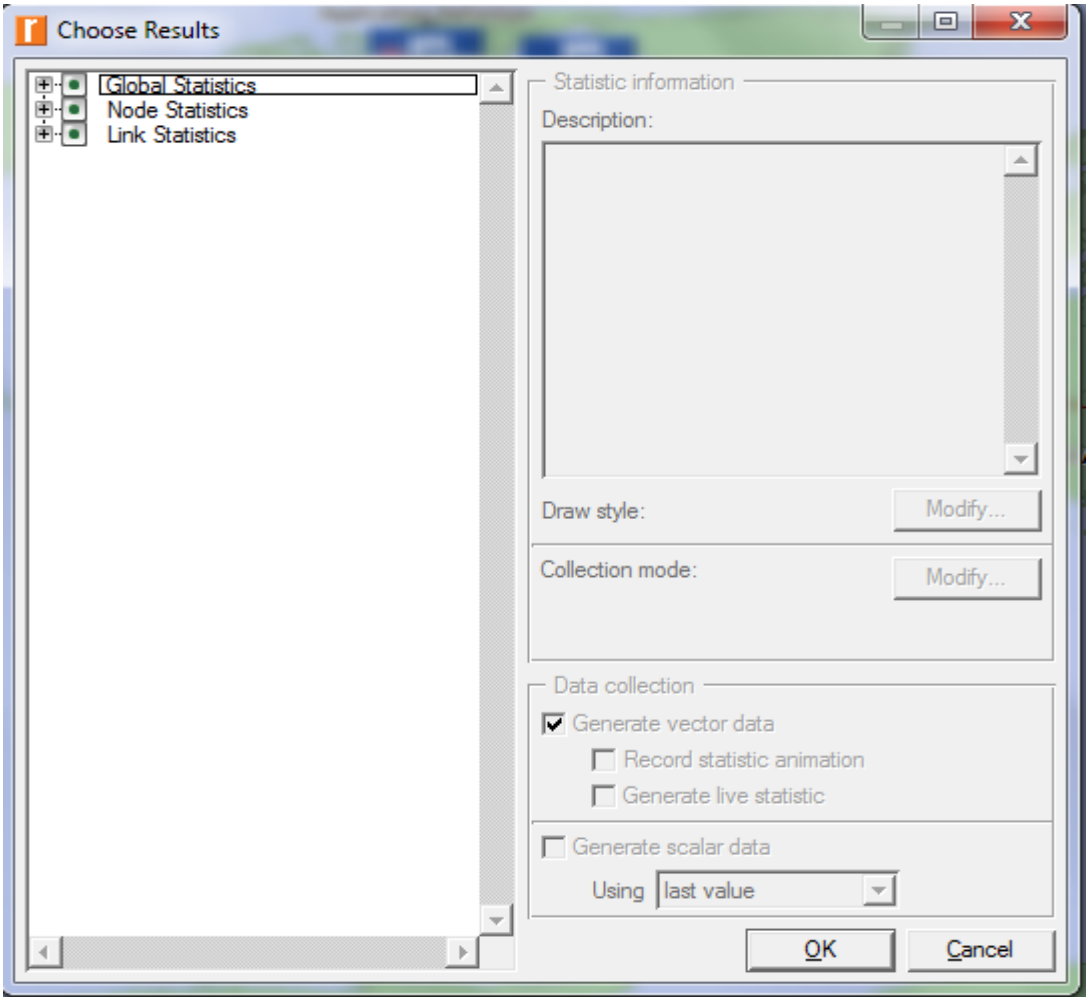



**Figure 3.18 Performance metrics**

Following metrics are chosen for performance evaluation. From the Global level statistics,

i. Expand the DB query option and choose response time, traffic sent and received

ii. Expand the HTTP option and choose the page response time, traffic sent and traffic received

iii. Also the download and upload response time, traffic sent and received options are checked for FTP options.

iv. Expand and select the Ethernet delay

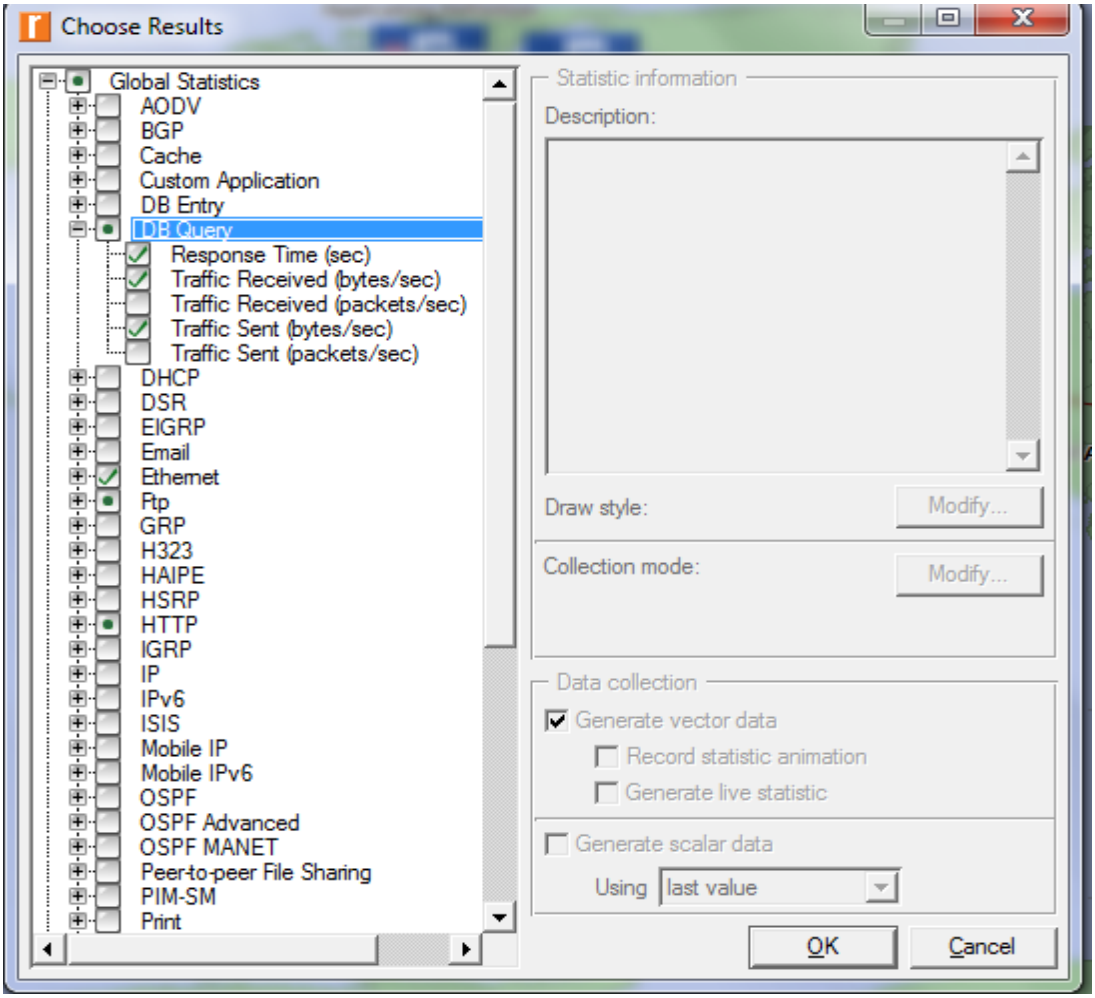



**Figure 3.19 Global Statistics Performance Metrics**

From the link level statistics the following metrics are selected

i. Expand point to point and select inbound and outbound utilization.

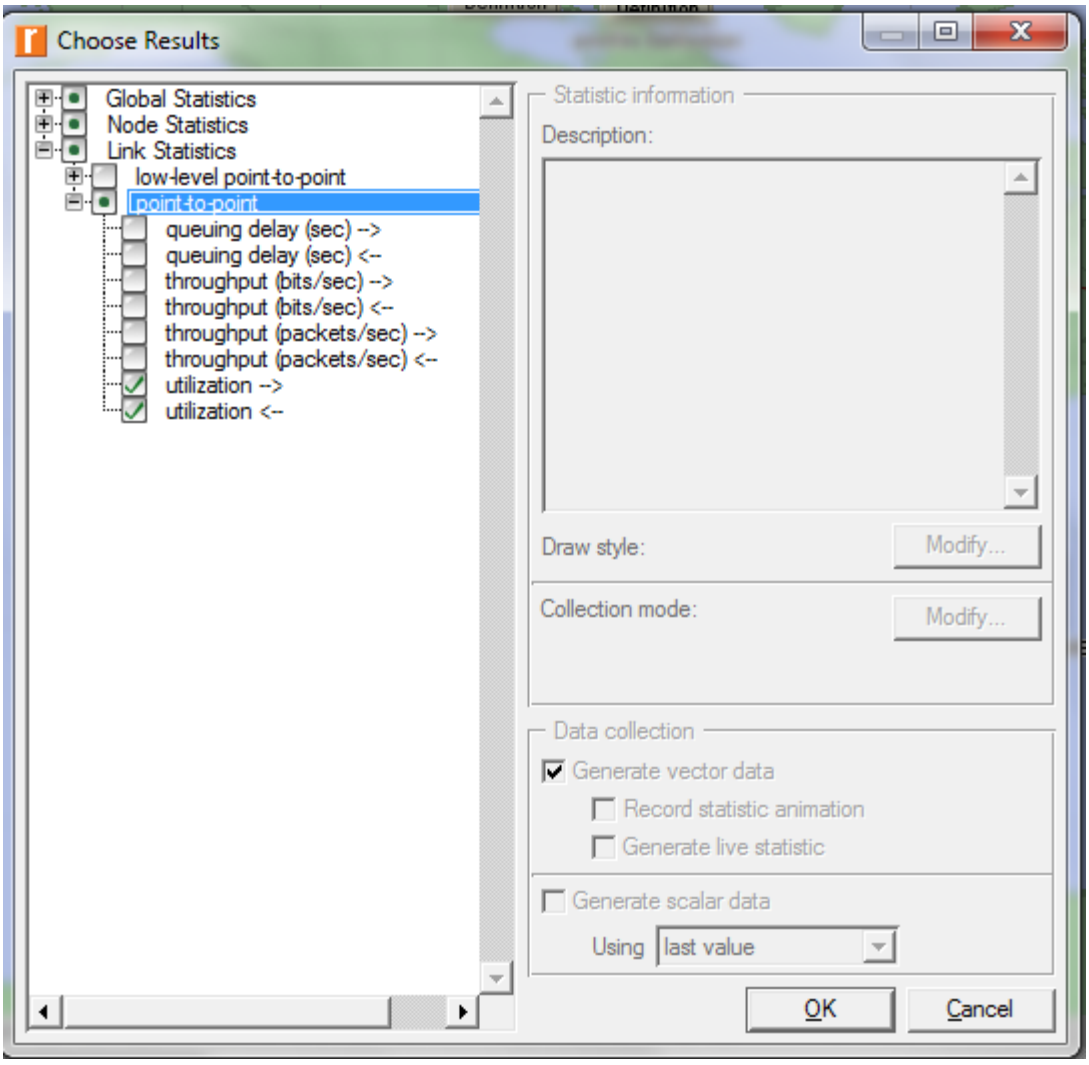



**Figure 3.20 Link level**

The performance metrics for the first scenarios is done. The next section explains the next scenario.

### 3.4.9 Simulation of Limited Security Scenario

Duplication of the no security scenario to create the new scenario for this section is done. In this scenario the Ethernet2_slip_8 firewall replaces Router 2 over the internet. The firewall will permit needed traffic to travel through the network and also perform packet filtering. The duplicate procedure is shown in Figure 3.20

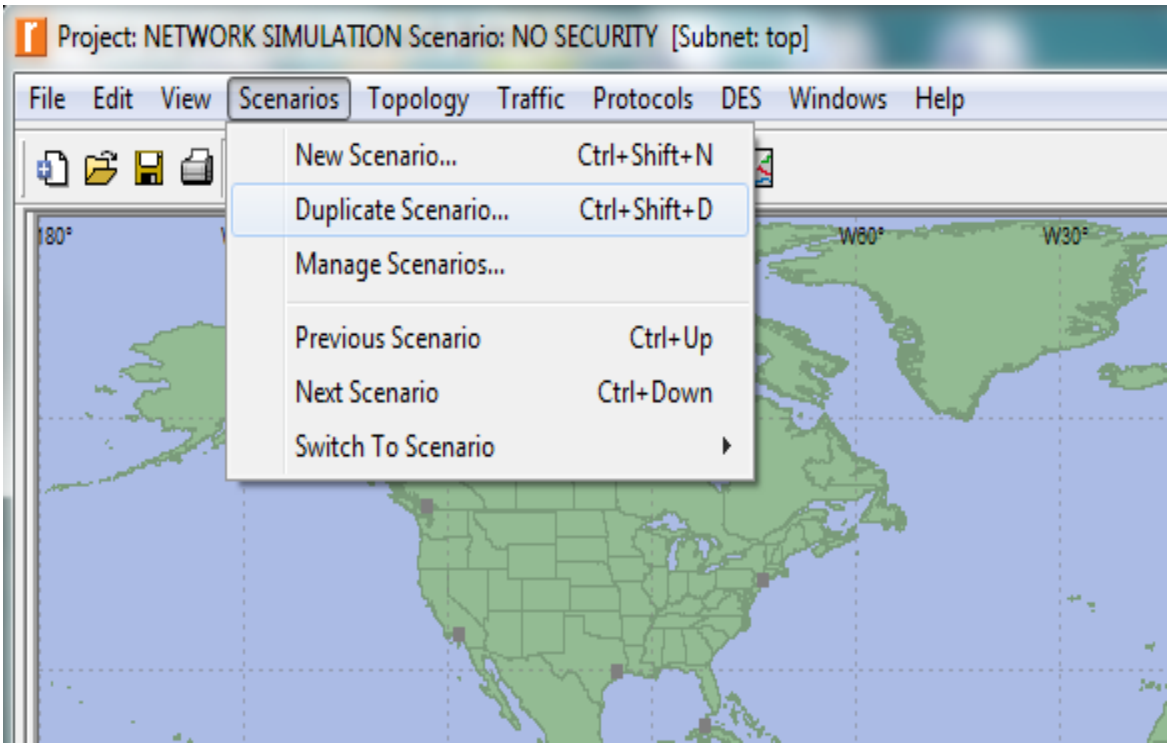



**Figure 3.21 Duplicate Scenario**

The steps below is used to configure the firewall

i. Remove Router 1 and replace with ethernet2_slip8_firewall

ii. Right click on the firewall and set its name to Limited Security setup and choose Edit attributes

iii. Expand Proxy server information and modify the “row 4” and set its latency value to a constant of 0.5

iv. Expand the row1, row3 and row 4 and set a constant of 0.05 as their latency.

A constant value of 0.05 is set for latency on database, file and web application which is an indication that, the firewall is performing packet filtering and thus a delay of 0.05 seconds is imposed over the router. A conceptual diagram of the network is as shown in Figure 3.22

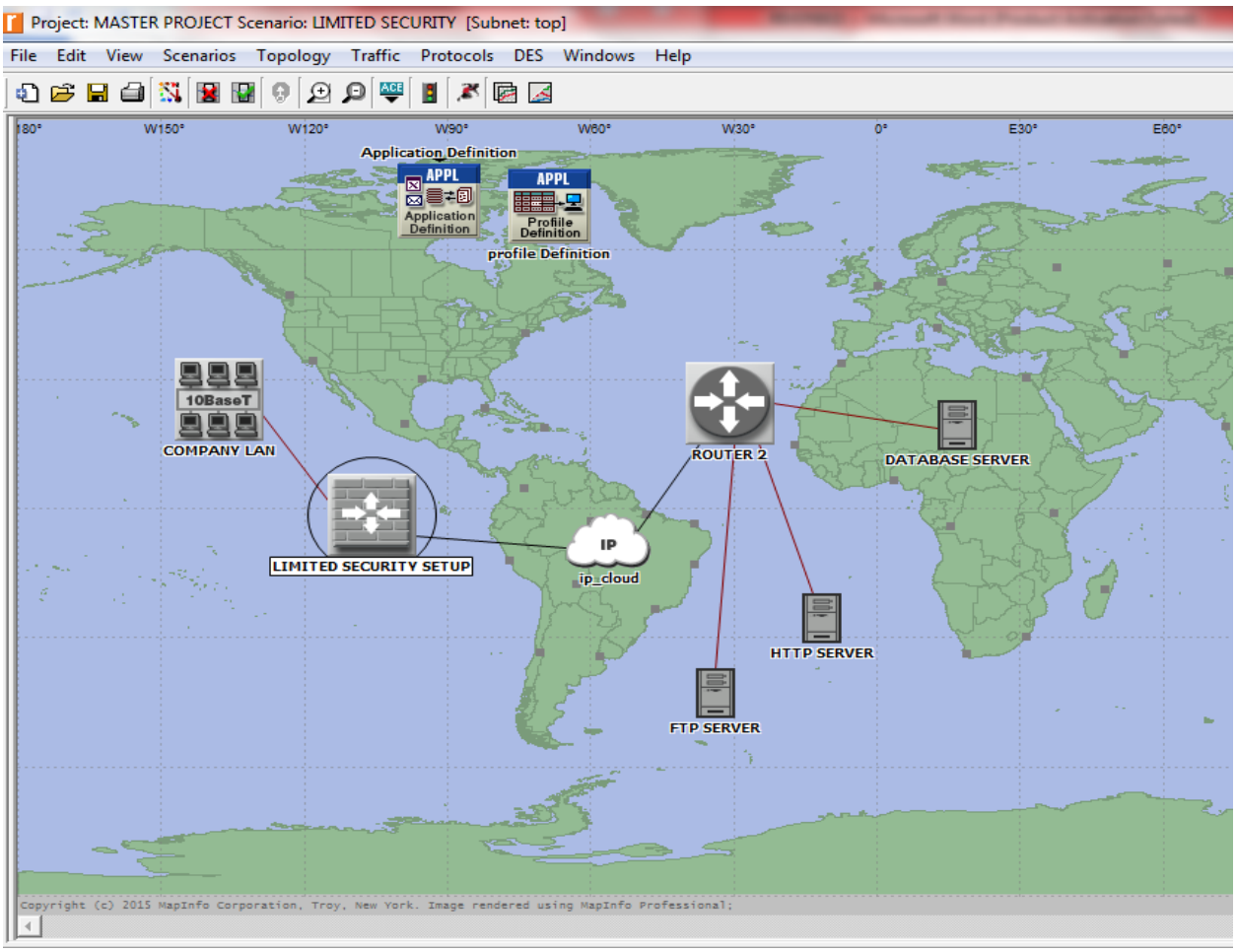



**Figure 3.22 Limited security scenario**

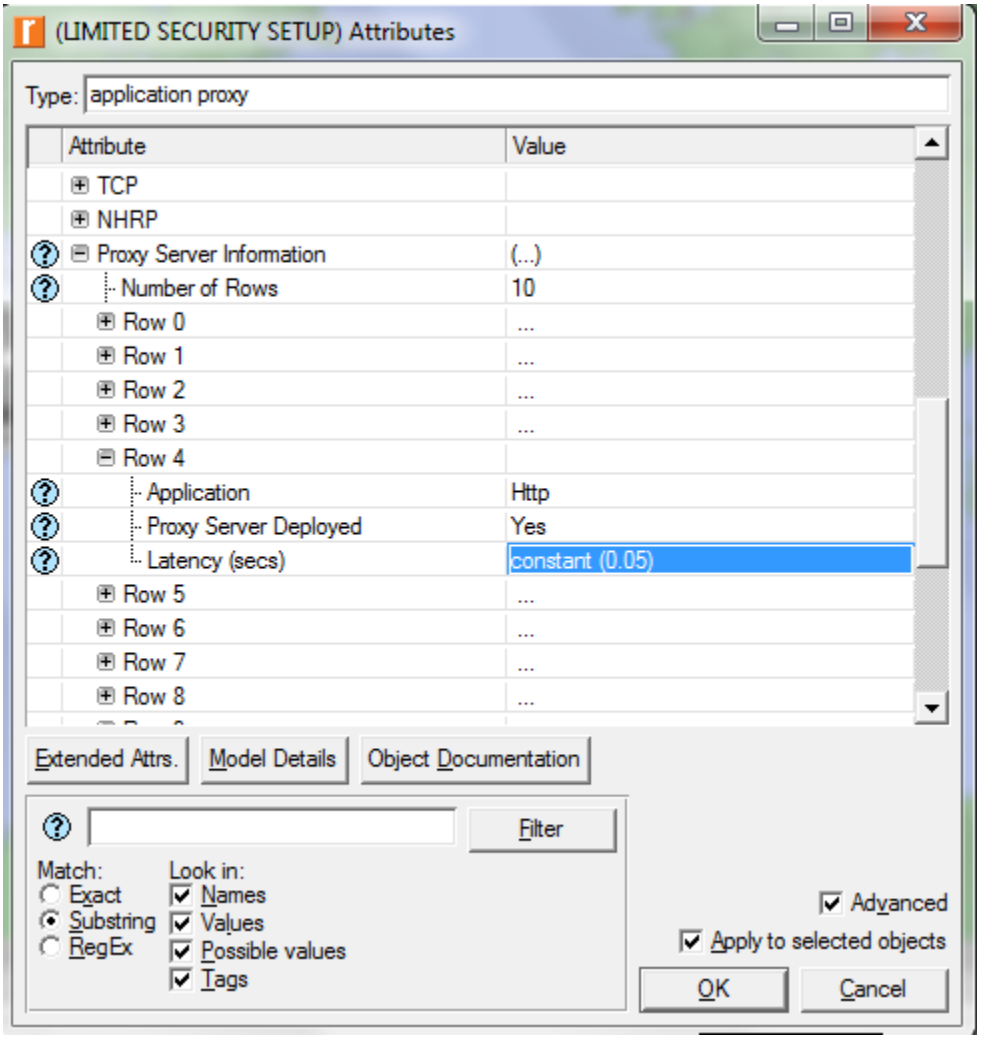



**Figure 3.23 Limited security setup configuration**

In the simulation, Limited security scenario is configured and the same performance metrics as the first scenario are used across this scenario.

### 3.4.10 Simulation of Advance security Scenario

In this scenario web traffic that travels through the network is obstructed. The scenario is designed by duplicating the second scenario. The following steps describe the changes are made to this network scenario:

i. Right click on ethernet2_slip8_firewall and set its name to Advance security setup and edit the attributes

ii. Expand the Proxy server information and select the row 4 which is HTTP application

iii. Change “proxy server deployed” to “No” as shown in Figure 3.25

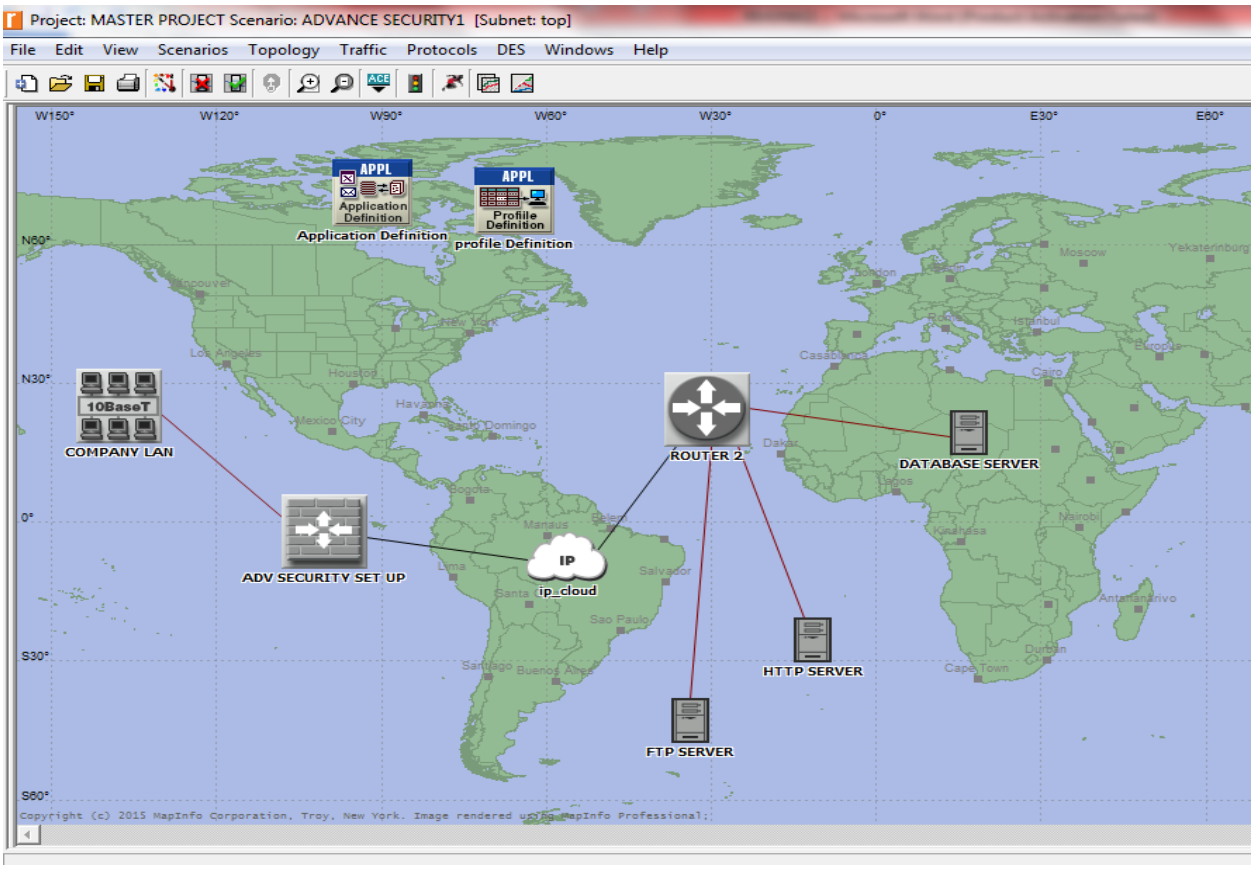



**Figure 3.24 Advance security scenario**

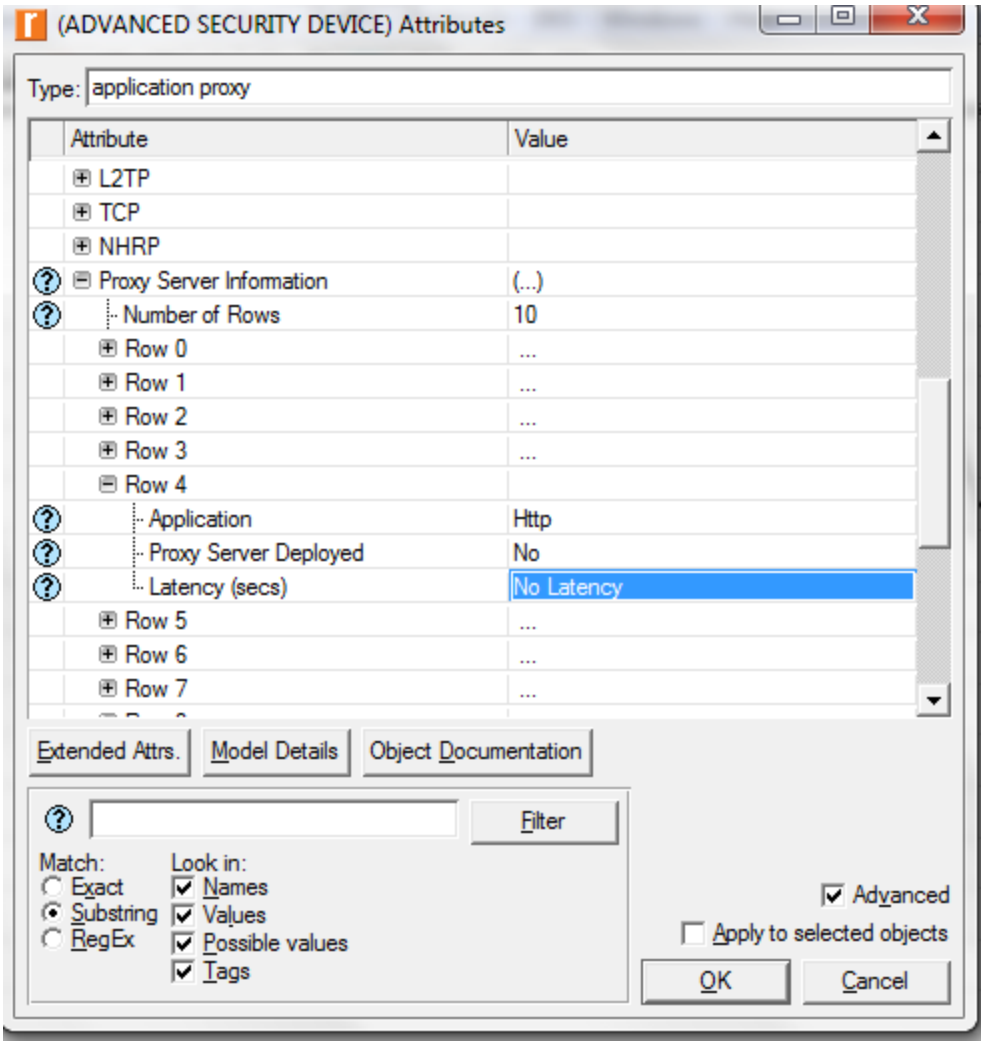



**Figure 3.25 Advanced security configuration**

With this all the HTTP traffic across the cloud is blocked for some users and enhances the simulation of Advanced Security Scenario.

### 3.5 Running the Simulation

After configuring the scenarios, the simulation is run for one hour. This is done by selecting the "manage scenarios" option from the scenario menu as displayed in figure 3.20

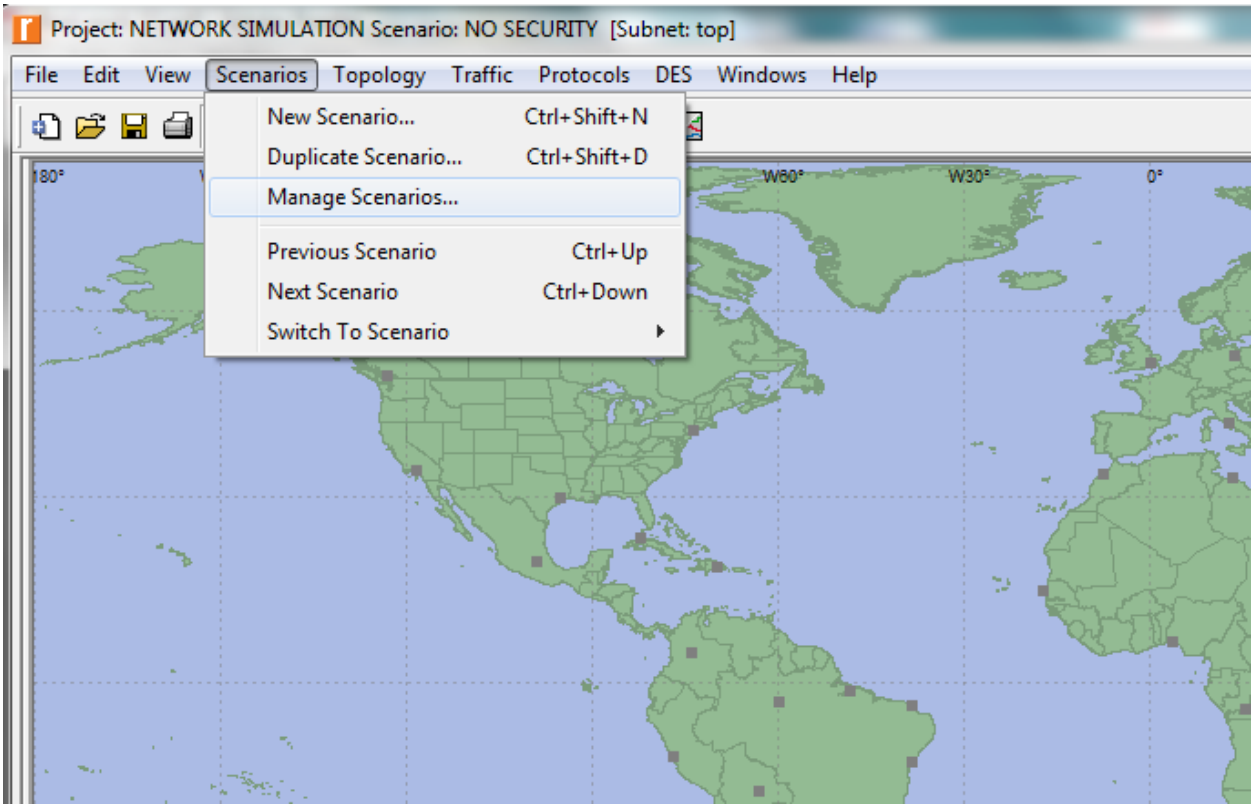



**Figure 3.26 Manage scenario**

By selecting the manage scenario, a new window opens which allows the simulation to run for one hour or more as depicted in Figure 3.27

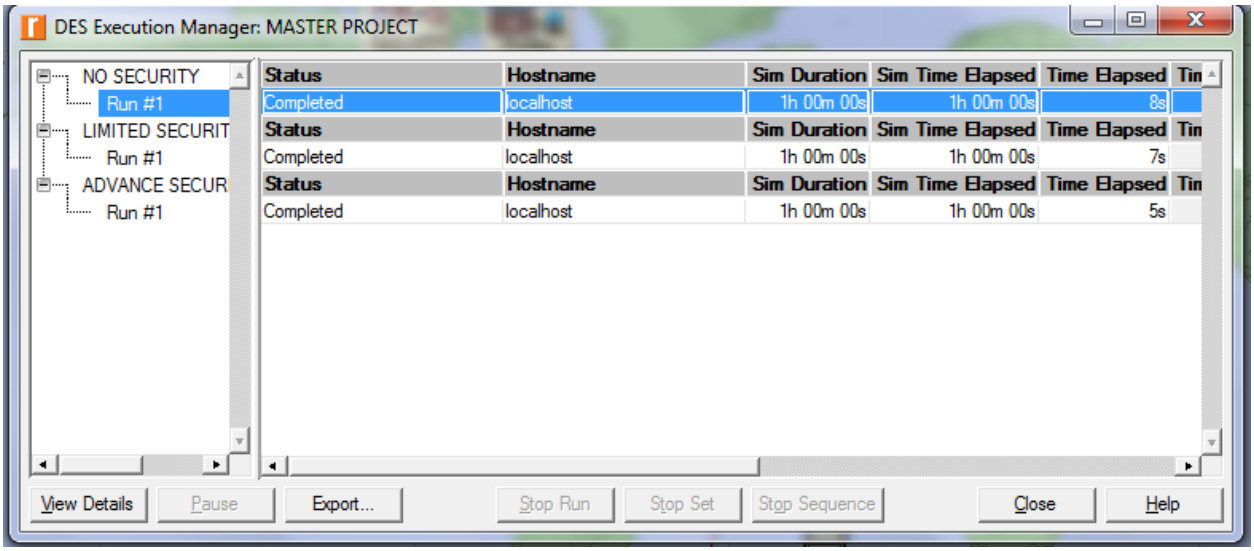



**Figure 3.27 Running simulation**

After the simulation is completed the result is analyzed and a detailed evaluation of results is done in chapter 4. A comparison is made between all the scenarios based on the performance metrics chosen.

# CHAPTER FOUR

# ANALYSIS AND IMPLEMENTATION

## 4.1 Introduction

This chapter analyses and discusses the results of the simulation in chapter 3. The analysis and discussions are evaluated after running the simulation for one hour. The three simulations in this research work are:

i. No Security scenario where there is no protection on the network. Hence all traffic generated from all the applications are permitted to pass through the router without any restriction.

ii. Limited Security scenario where a firewall is installed on the network to filter packets of the three applications.

iii. The Advance Security scenario where firewall is imposed with blocking capabilities to block one application. Traffic from HTTP application is blocked for some users in the company whiles that of Database and FTP applications are allowed to pass through.

The tables in section 4.2 shows the results of the simulation experiment conducted in chapter 3.

## 4.2 Result of the Simulation Experiment

The outcomes of the simulations for all the scenarios are presented in this section. The Tables below shows the Ethernet delay, taking after the first 15 and 45 minutes of the simulation time with different switching speed and varying load.

### 4.2.1 Ethernet Delay Results

**Table 4.1 Ethernet delay with packet size of 10mb (low load)**

| ETHERNET DELAY LOW LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 0.031849 | 0.031752 | 0.031381 | 0.031368 | 0.031551 | 0.03146 |
| **LIMITED SECURITY** | 0.029708 | 0.029326 | 0.029755 | 0.029327 | 0.029975 | 0.029519 |
| **ADVANCED SECURITY** | 0.030193 | 0.029975 | 0.030192 | 0.029974 | 0.030245 | 0.030049 |

**Table 4.2 Ethernet delay with packet size of 50mb (medium load)**

| ETHERNET DELAY WITH MEDIUM LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gbps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 0.032 | 0.032 | 0.031 | 0.031 | 0.032 | 0.032 |
| **LIMITED SECURITY** | 0.029 | 0.029 | 0.029 | 0.029 | 0.029 | 0.029 |
| **ADVANCED SECURITY** | 0.033 | 0.033 | 0.033 | 0.033 | 0.033 | 0.033 |

**Table 4.3 Ethernet delay with packet size of 100mb (high load)**

| ETHERNET DELAY WITH HIGH LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gbps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 0.033 | 0.033 | 0.034 | 0.033 | 0.034 | 0.034 |
| **LIMITED SECURITY** | 0.030 | 0.029 | 0.031 | 0.030 | 0.034 | 0.035 |
| **ADVANCED SECURITY** | 0.034 | 0.035 | 0.035 | 0.034 | 0.035 | 0.034 |

### 4.2.2 HTTP page response time

The Tables below show the HTTP page response time, taking after the first 15 and 45 minutes of the simulation time with different switching speed.

**Table 4.4 HTTP page response time with packet size of 10mb (low load)**

| HTTP PAGE RESPONSE WITH LOW LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 0.751008 | 0.753608 | 0.72876 | 0.740808 | 0.750731 | 0.724027 |
| **LIMITED SECURITY** | 0.508485 | 0.496347 | 0.504508 | 0.508169 | 0.496803 | 0.504206 |
| **ADVANCED SECURITY** | 0.152309 | 0.149915 | 0.152308 | 0.149914 | 0.109388 | 0.125983 |

**Table 4.5 HTTP page response time with packet size of 50mb (medium load)**

| HTTP PAGE RESPONSE WITH MEDIUM LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gbps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 0.503788 | 0.50579 | 0.470836 | 0.495626 | 0.499494 | 0.499539 |
| **LIMITED SECURITY** | 0.477433 | 0.50588 | 0.490998 | 0.497054 | 0.489484 | 0.502342 |
| **ADVANCED SECURITY** | 0.128929 | 0.133095 | 0.1402 | 0.128689 | 0.130938 | 0..140456 |

**Table 4.6 HTTP page response time with packet size of 100mb (high load)**

| HTTP PAGE RESPONSE WITH HIGH LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gbps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 14.4188 | 15.16266 | 13.15442 | 14.56281 | 14.16418 | 15.58603 |
| **LIMITED SECURITY** | 9.971854 | 11.15779 | 9.82973 | 11.05133 | 4.339151 | 3.503513 |
| **ADVANCED SECURITY** | 0.123074 | 0.13841 | 0.1317 | 0.123679 | 0.150175 | 0.146801 |

### 4.2.3 FTP downloads response time

The Tables below shows the FTP download and upload results, taking after the first 15 and 45 minutes of the simulation time with different switching speed

**Table 4.7 FTP downloads response time with packet size 10mb (low load)**

| FTP DOWNLOAD RESPONSE TIME 10MB (LOW LOAD) | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 0.183463 | 0.130961 | 0.07721 | 0.144607 | 0.194266 | 0.220272 |
| **LIMITED SECURITY** | 0.388105 | 0.432882 | 0.25342 | 0.347535 | 0.441276 | 0.393998 |
| **ADVANCED SECURITY** | 0.264058 | 0.28095 | 0.264053 | 0.280945 | 0.342098 | 0.417238 |

**Table 4.8 FTP downloads response time with packet size 50mb (medium load)**

| FTP DOWNLOAD RESPONSE TIME MEDIUM LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gbps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 0.232 | 0.197 | 0.191 | 0.166 | 0.232 | 0.197 |
| **LIMITED SECURITY** | 0.425 | 0.470 | 0.509 | 0.522 | 0.481 | 0.497 |
| **ADVANCED SECURITY** | 0.504 | 0.525 | 0.535 | 0.565 | 0.465 | 0.488 |

**Table 4.9 FTP downloads response time with packet size 100mb (high load)**

| FTP DOWNLOAD RESPONSE TIME HGH LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gbps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 5.594 | 4.654 | 6.327 | 5.202 | 7.262 | 5.324 |
| **LIMITED SECURITY** | 26.259 | 35.761 | 31.214 | 35.679 | 11.064 | 8.064 |
| **ADVANCED SECURITY** | 1.187 | 1.093 | 1.216 | 1.084 | 1.087 | 1.086 |

### 4.2.4 FTP uploads response time

The Tables below show the FTP upload response time, taking after the first 15 and 45 minutes of the simulation time with different switching speed.

**Table 4.10 FTP upload response time with packet size 10mb(low load)**

| FTP UPLOAD RESPONSE TIME 10MB (LOW LOAD) | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 0.11026 | 0.224611 | 0.162853 | 0.219477 | 0.090653 | 0.165794 |
| **LIMITED SECURITY** | 0.262592 | 0.309749 | 0.48156 | 0.471822 | 0.315871 | 0.327106 |
| **ADVANCED SECURITY** | 0.340902 | 0.337859 | 0.340897 | 0.337854 | 0.267664 | 0.315456 |

**Table 4.11 FTP upload response time with packet size 50mb (medium load)**

| FTP UPLOAD RESPONSE TIME MEDIUM LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gbps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 0.320 | 0.323 | 0.320 | 0.328 | 0.320 | 0.323 |
| **LIMITED SECURITY** | 0.689 | 0.728 | 0.731 | 0.760 | 0.722 | 0.733 |
| **ADVANCED SECURITY** | 0.730 | 0.777 | 0.655 | 0.731 | 0.820 | 0.728 |

**Table 4.12 FTP upload response time with packet size 100mb (high load)**

| FTP UPLOAD RESPONSE TIME HIGH LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gbps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 3.774 | 4.636 | 6.365 | 4.087 | 1.243 | 2.535 |
| **LIMITED SECURITY** | 30.854 | 34.466 | 28.806 | 34.492 | 11.067 | 9.238 |
| **ADVANCED SECURITY** | 1.378 | 1.361 | 1.417 | 1.398 | 1.359 | 1.357 |

### 4.2.5 Database query response time

The Tables below show the database query response time, taking after the first 15 and 45 minutes of the simulation time with different switching speed and varying load.

**Table 4.13 Database query response time with packet size 10mb (low load)**

| DATABASE QUERY RESPONSE TIME 10MB (LOW LOAD) | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 0.21092 | 0.210061 | 0.176882 | 0.175817 | 0.1726 | 0.175538 |
| **LIMITED SECURITY** | 0.094278 | 0.093375 | 0.095171 | 0.097574 | 0.085625 | 0.087546 |
| **ADVANCED SECURITY** | 0.032681 | 0.032914 | 0.03268 | 0.032912 | 0.030425 | 0.031861 |

**Table 4.14 Database query response time with packet size of 50mb(medium load)**

| DATABASE QUERY RESPONSE TIME WITH MEDIUM LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | **5Mbps** | | **1Gbps** | | **5Gbps** | |
| **SIMULATION TIME** | **15MINS** | **45MINS** | **15MINS** | **45MINS** | **15MINS** | **45MINS** |
| **NO SECURITY** | 0.136 | 0.138 | 0.142 | 0.144 | 0.136 | 0.138 |
| **LIMITED SECURITY** | 0.087 | 0.087 | 0.089 | 0.090 | 0.106 | 0.108 |
| **ADVANCED SECURITY** | 0.011 | 0.012 | 0.012 | 0.012 | 0.011 | 0.012 |

**Table 4.15 Database query response time with packet size of 100mb (high load)**

| DATABASE QUERY RESPONSE TIME WITH HIGH LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | **5Mbps** | | **1Gbps** | | **5Gbps** | |
| **SIMULATION TIME** | **15MINS** | **45MINS** | **15MINS** | **45MINS** | **15MINS** | **45MINS** |
| **NO SECURITY** | 61.176 | 173.367 | 33.301 | 90.054 | 64.068 | 185.918 |
| **LIMITED SECURITY** | 20.515 | 50.578 | 20.674 | 47.989 | 2.654 | 1.790 |
| **ADVANCED SECURITY** | 0.135 | 0.136 | 0.136 | 0.136 | 0.135 | 0.136 |

### 4.2.6 Database traffic received

The Tables below shows the database query traffic received, taking after the first 15 and 45 minutes of the simulation time with different switching speed.

**Table 4.16 Database traffic received with packet size 10mb (low load)**

| **DATABASE TRAFFIC RECEIVED 10MB (LOW LOAD)** | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 2078.701 | 2192.655 | 2038.667 | 2144.228 | 2020.615 | 2161.404 |
| **LIMITED SECURITY** | 2050.513 | 2156.579 | 2062.342 | 2155.035 | 2030.769 | 2133.228 |
| **ADVANCED SECURITY** | 2020.598 | 2174.526 | 2020.598 | 2174.526 | 1981.692 | 2141.333 |

**Table 4.17 Database traffic received with packet size off 50mb (medium load)**

| **DATABASE QUERY TRAFFIC RECIEVED WITH MEDIUM LOAD** | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | **5Mbps** | | **1Gbps** | | **5Gbps** | |
| **SIMULATION TIME** | **15MINS** | **45MINS** | **15MINS** | **45MINS** | **15MINS** | **45MINS** |
| **NO SECURITY** | 9581.95 | 10338.43 | 9637.20 | 10350.41 | 9581.95 | 10338.43 |
| **LIMITED SECURITY** | 9578.67 | 10356.40 | 9489.50 | 10283.42 | 9586.87 | 10424.89 |
| **ADVANCED SECURITY** | 9511.38 | 10303.63 | 9516.85 | 10294.27 | 9490.60 | 10244.12 |

**Table 4.18 Database query traffic received with packet size of 100mb (high load)**

| **DATABASE QUERY TRAFFIC RECIEVED WITH HIGH LOAD** | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | **5Mbps** | | **1Gbps** | | **5Gbps** | |
| **SIMULATION TIME** | **15MINS** | **45MINS** | **15MINS** | **45MINS** | **15MINS** | **45MINS** |
| **NO SECURITY** | 265377.37 | 289353.17 | 282992.14 | 311672.51 | 258050.19 | 281738.67 |
| **LIMITED SECURITY** | 293529.16 | 320590.04 | 292915.42 | 321714.90 | 310587.08 | 338274.99 |
| **ADVANCED SECURITY** | 310294.43 | 334174.88 | 315842.74 | 337860.49 | 314524.99 | 336984.51 |

### 4.2.7 Database query traffic sent

The Tables below show the database query traffic sent, taking after the first 15 and 45 minutes of the simulation time with different switching speed.

**Table 4.19 Database query traffic sent with packet size of 10mb (low load)**

| DATABASE TRAFFIC SENT 10MB (LOW LOAD) | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | 5Mbps | | 1Gbps | | 5Gps | |
| **SIMULATION TIME** | 15MINS | 45MINS | 15MINS | 45MINS | 15MINS | 45MINS |
| **NO SECURITY** | 2078.718 | 2192.667 | 2039.761 | 2144.228 | 2020.615 | 2161.965 |
| **LIMITED SECURITY** | 2050.513 | 2156.579 | 2062.906 | 2155.035 | 2031.316 | 2133.228 |
| **ADVANCED SECURITY** | 2035.932 | 2192.304 | 2035.932 | 2192.304 | 1999.744 | 2159.673 |

**Table 4.20 Database query traffic sent with packet size of 50mb (medium load)**

| DATABASE QUERY TRAFFIC SENT WITH MEDIUM LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | **5MB** | | **1GB** | | **5GB** | |
| **SIMULATION TIME** | **15MINS** | **45MINS** | **15MINS** | **45MINS** | **15MINS** | **45MINS** |
| **NO SECURITY** | 9582.50 | 10338.62 | 9637.20 | 10350.41 | 9582.50 | 10338.62 |
| **LIMITED SECURITY** | 9579.21 | 10356.77 | 9489.50 | 10283.42 | 9587.97 | 10425.26 |
| **ADVANCED SECURITY** | 9511.38 | 10303.63 | 9516.85 | 10294.27 | 9490.60 | 10244.12 |

**Table 4.21 Database query traffic sent with packet size of 100mb (high load)**

| DATABASE QUERY TRAFFIC SENT WITH HIGH LOAD | | | | | | |
|---|---|---|---|---|---|---|
| **SWITCHING SPEED** | **5MB** | | **1GB** | | **5GB** | |
| **SIMULATION TIME** | **15MINS** | **45MINS** | **15MINS** | **45MINS** | **15MINS** | **45MINS** |
| **NO SECURITY** | 317128.21 | 337754.39 | 310658.19 | 335076.30 | 311899.90 | 335588.87 |
| **LIMITED SECURITY** | 308344.34 | 335539.09 | 309376.00 | 333920.94 | 311182.22 | 338347.23 |
| **ADVANCED SECURITY** | 310329.44 | 334198.83 | 315947.76 | 337872.47 | 314560.00 | 336996.68 |

These are the results of the simulation. In the next sections, these results will be analyzed and discussed.

The performance of the database, HTTP and FTP application are discussed in graphical representation based on the performance metrics chosen at the global level statistics. All the obtained graphs are compared against the performance metrics and a detailed analysis is given.

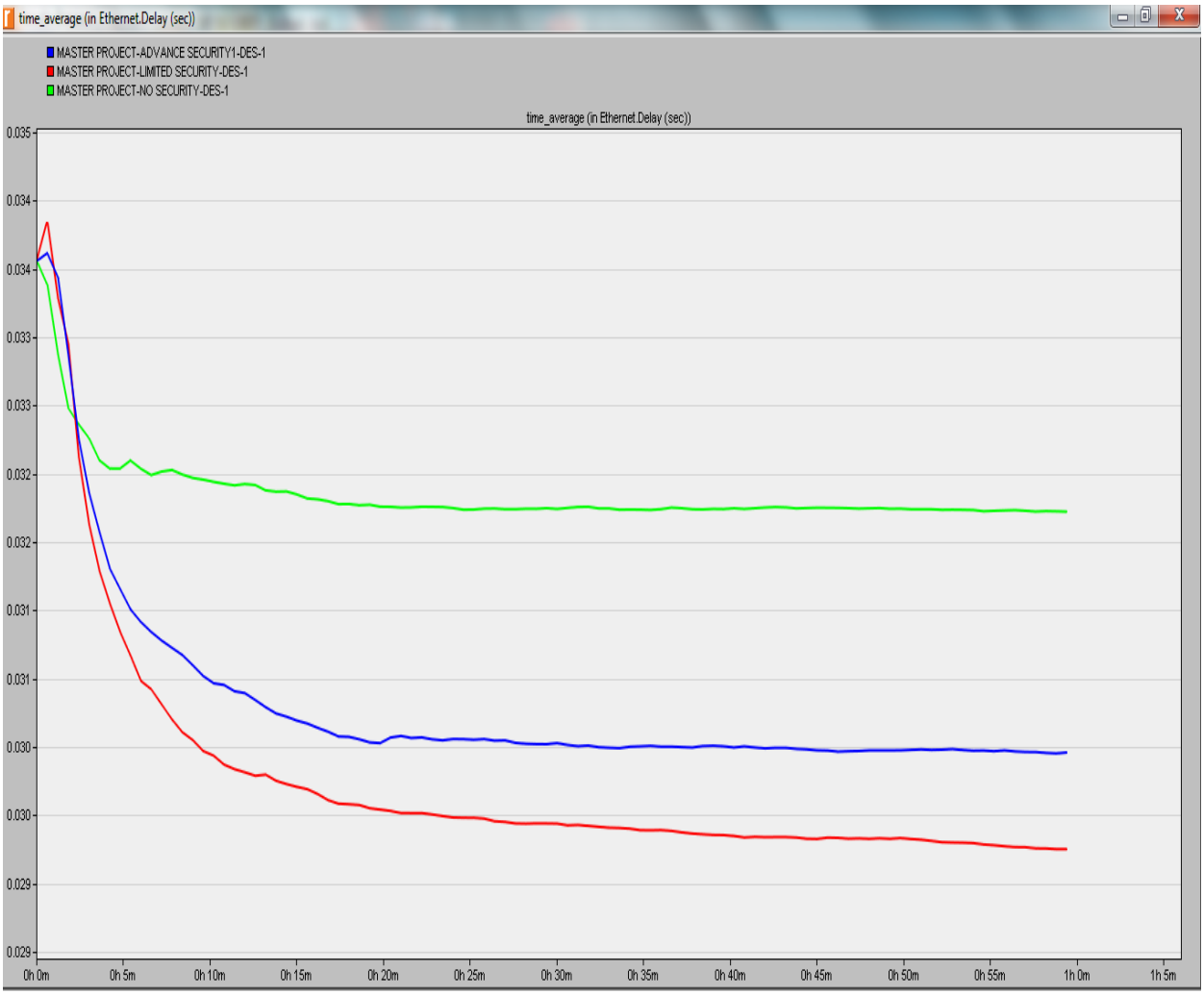
### 4.3 Analysis on Ethernet delay (latency)

Ethernet delay point out to be one key indicator to ascertain the performance of the network. In this research, latency refers to the amount of time spent between sending and receiving information over a public-shared network. Ethernet delay of packets is the delay from the time of the start of packet transmission at the sender host to the time of the end of packet reception at the receiver host. Generally, the total application latency is a measure of the time taken to process information at both the sending and receiving hosts (host latency) and the delays which takes place inside the network (network latency). Total latency= host latency +network latency.

However delay may vary slightly base on the location of each node on the network. Again it may differ also based on the amount of traffic that goes through the network.

### 4.3.1 Ethernet delay

**Ethernet delay(bits/sec)**




**Simulation time(mins)**

**Figure 4. 1 Ethernet delay**

Figure 4.1 measures the total delay on the network. When no illicit traffic was blocked, Tables 4.1 to 4.3 shows the varied results for 10mb 50mb and 100mb network load which was imposed on the network with link speed of 500mbps, 1gbps and 5gbps. When the network was run for the first 15 minutes with data rate of 500mbps it could be realized that delay from Tables 3.1 was 0.034 and was dropped to 0.031 after the first 15 minutes and remained steadily through to the

45th minute of the simulation. This shows that there are no significant changes in the network delay when there was no security on the network. However, the network latency increases with increasing load on the network

### 4.3.2 Ethernet delay- Limited security

From Table 4.1 the values of 0.029708 and 0.029326 of the same table with varying load, the delay for the network also remained constant after the first 15 minutes to the end of simulation. It also clearly show that the value of network delay is deterministic whenever there is no or limited security on the network as delay drops from 0.034 at the start of simulation to 0.029 and remained constant till the end of the simulation.

### 4.3.3 Ethernet delay-Advance security

Comparably, Ethernet delay remained lower at 0.029 when there was limited security as against a high value of 0.030 for advanced security. This is due to the fact that with limited security the firewall imposed on the network was doing only packet filtering as compared to that of advanced security which was doing packet filtering with application blocking. These activities of the firewall cause the advanced security to have a high delay as compared to the limited security.

However with no security on the network, the delay was higher thus 0.0317 resulting from high and frequent access of the network from both authorized and unauthorized users which may subject the network to series of attacks such as denial of service attack, man in the middle attack and many more cause high delay in the network.

Generally it could be clearly observed from the experiment that,

i. Increasing data packets increases delay in the network

ii. Network delay decreases when the simulation is started and remains constant later throughout the simulation period.

### 4.4 Analysis on Database applications

The database application is one of the applications that was used to generated traffic in this experiment and the performance of the database application is estimated against the database query response time, database traffic received and database traffic sent. A packet size of 10MB (low), 50MB(medium) and 100MB(high) are imposed across the network and a switching speed of 5Mbps, 1Gbps and 5Gbps are set between the router and the cloud. The database query response, database traffic sent and received times are evaluated with each packet sizes and data rate to investigate applications performance. This section discusses the performance evaluation of the database application under the three scenarios. Database Query Response Time is the elapsed time between the end of an inquiry, query or demand on a computer system (e.g. Database server) and the beginning of a response; for example, the length of the time between an indication of the end of an inquiry and the display of the first character (result) of the response at a user terminal. Lower the query response time indicates higher performance of the database application.

### 4.4.1 Database query response time- No security

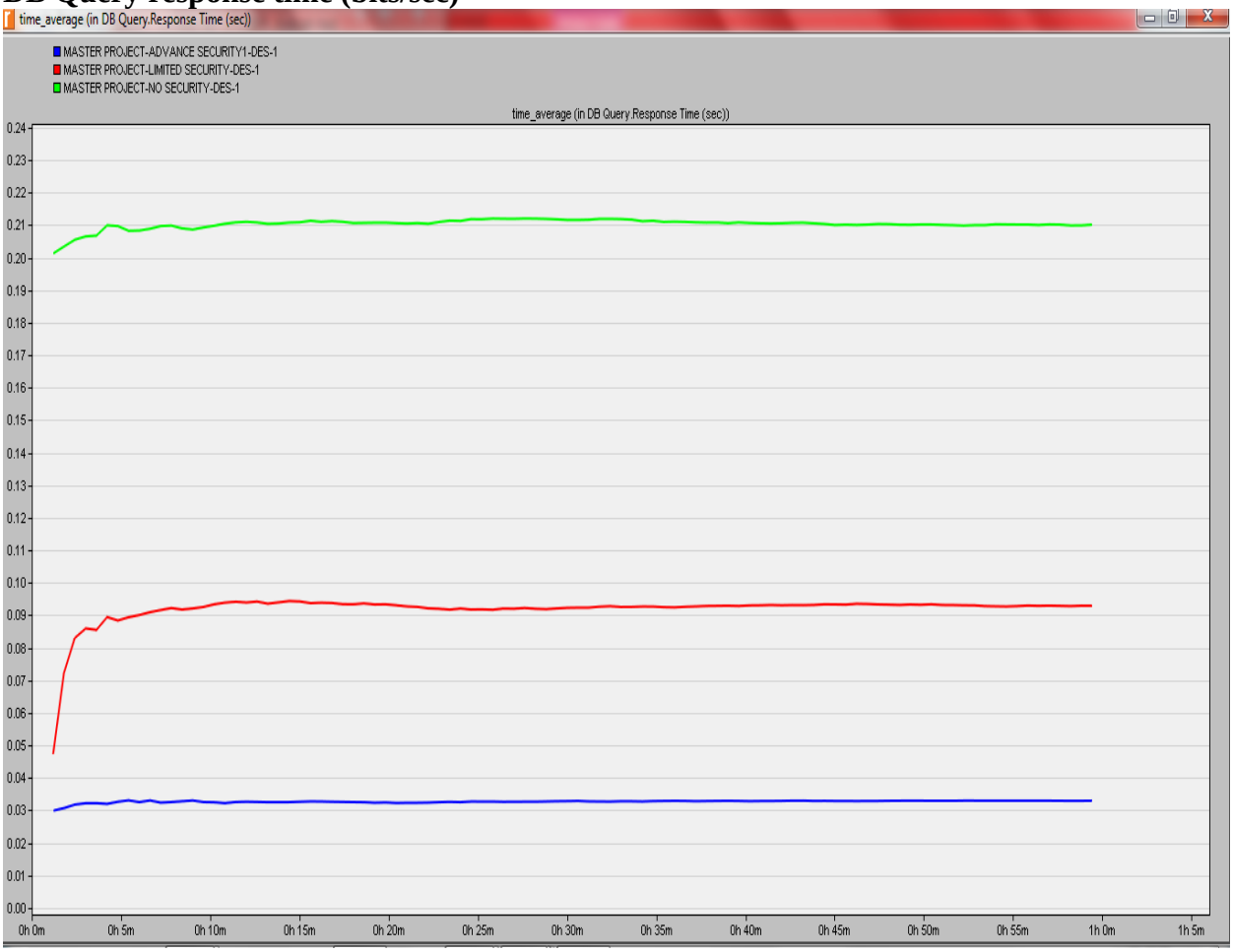



**Figure 4. 2 Database query response time**

From Figure 4.2 No security scenario allows all the applications to pass through the network without any limitations and restrictions to the flow of traffic. Concerning database query the lower the database query response time the faster the query response. Tables 4.13-4.15 give details of the database query response time.

It can be observed from the Tables that, the query response time has a higher value of 0.21 seconds when no restrictions is imposed on the network with the packet size is 10MB as

compared to the other two scenarios with lower response time. But from the graph it could be seen that throughout the simulations the response time was not stable as it kept on moving up and down between 0.20012 and 0.21092 from start of simulation to end of simulation. It shows an instability in query response time when no security is configure on the network. However it is a clear indication that when there is no security measures on a network the network becomes susceptible to replay attacks which in turn cause some delay in the network when the database is queried. Table 4.15 also shows that as the load on the network increases for no security in place the database query response time skewed higher and reaching 61.17565. It can therefore be best explained that as the load increase the slower the response time when database is queried.

### 4.4.2 Database query response time -Limited security

Following Figure 4.2 and the values on Tables 4.13 it could be gathered that 0.094 was the value recorded for limited security when packet size of 10mb traversed the network at a speed of 500mbps. The graph in the figure below shows the database query response time rose from 0.049 from start of simulation to 0.0942 after 15 minutes and remained steadily till the end of the simulation.

### 4.4.3 Database query response time advance security

HTTP applications, consumes more bandwidth on the internet causing the network to be slow. Here, HTTP traffic was block for some users on the network reducing the amount of network traffic. Hence when the database application was queried it showed a lower response time of 0.0329 which is a clear indication that maximizing security with by blocking some applications on the network enhances a very good response time when the database is queried. As the load on the network increases to 100mb, it could be gathered that the database query response time change from 0.011416 when 10mb was imposed to 0.135318 which is not even up to 0.1%

increase as compared to that of the other two scenarios. From these facts, it can be established that HTTP applications consumes bandwidth on the network more than any other application on the network. Figure 4.2 gives a graphical representation of the analysis.

### 4.5 Analysis on Database traffic received or sent

The database traffic received or sent records the total amount of OSPF traffic received or sent across all connected interfaces of all nodes of the network. The statistics are available in unit of bits per seconds. These statistics are accumulated base on the types of OSPF messages which includes database description, hello, link state Acknowledgement (multicast), link state Acknowledgement (unicast), link state request, link state update (multicast), link state update (unicast). The higher the value of traffic received the better the network performance.

### 4.5.1 Database traffic received—NO security

**DB traffic received(bytes/sec)**

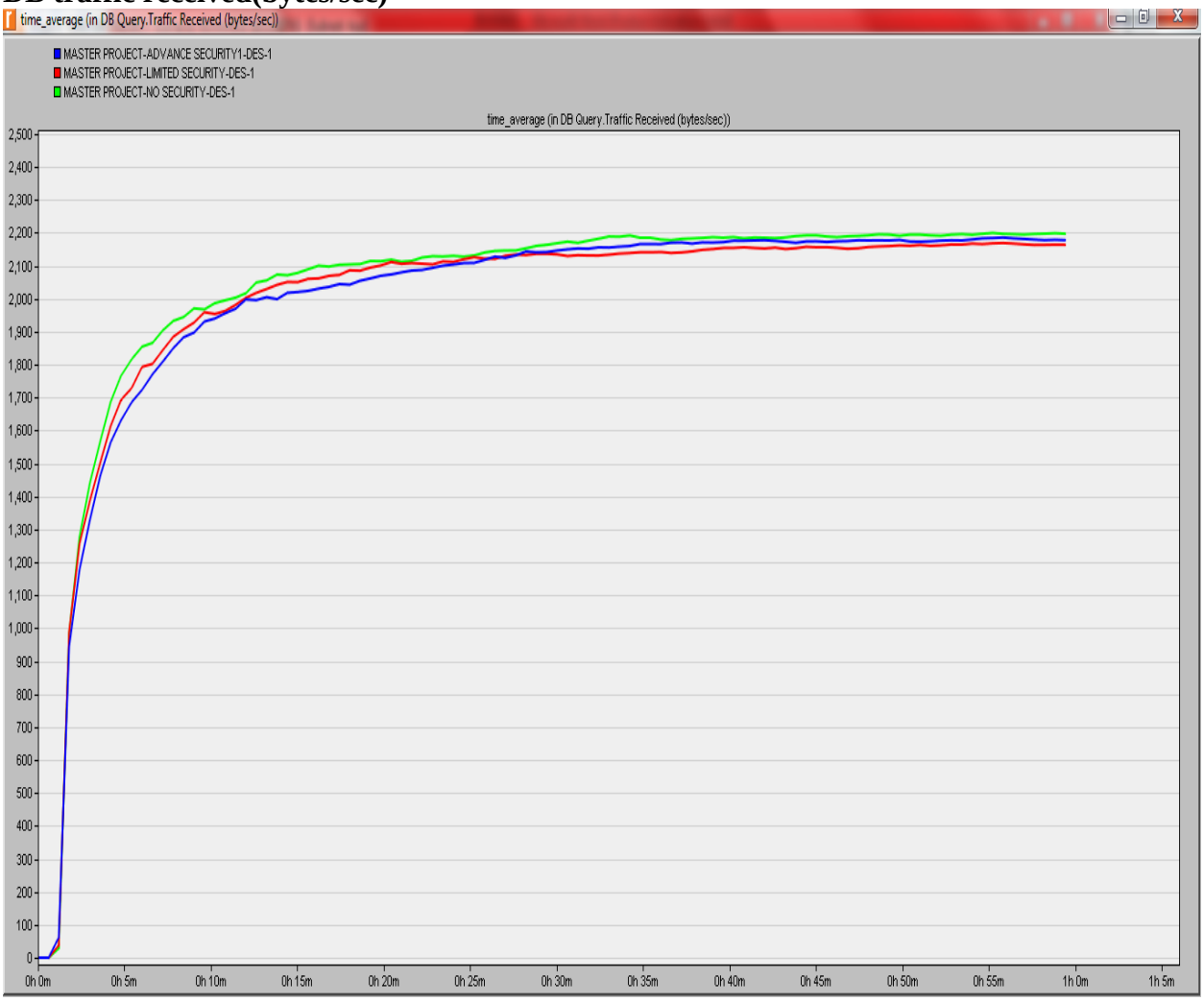



**Figure 4. 3 Database traffic received**

Following the Tables 4.16-4.18 with a low load of 10mb on the network, the database query traffic received started at 0.0011and appreciated greatly with increasing simulation time to a value of 2192.655 and remained constant afterwards throughout the simulation. The Figure 4.7 shows that there was rapid rise immediately the simulation was started from 0.0011 at 1 minute of simulation interval. Within that time the network was highly congested making it to work under stress condition. After reaching its peak, remains constant with some slim margin of

changes. It could also be noted that the database traffic received for no security scenario keeps increasing with increasing load on the network. Thus the more loads the more traffic received or sent. From the figures below it could be observed that no security, limited security and advanced security scenarios started at the same point and reached 2192.655, 2156.579, 2174.526 respectively after 45 minutes of the simulation and eventually move together till end of the simulation. It is a clear indication of no significant change in the traffic received for the three scenarios. It can therefore be explained that once nodes are connected on the network, traffic begins to flow through the network irrespective of the network being secured or not. However there is as there is a slim rise and fall in the amount of network traffic with an increase in switching speed of the network. On the contrary, the traffic increases immensely with increasing load. Tables 4.16 to 4.18 shows a clearly interpretation of Figure 4.3

### 4.5.2 Database traffic received—Limited security

Tables 4.16 -4.18 clearly shows the database query traffic received. Traffic through the network was skewed upwards with increasing switching speed. Thus from Tables 4.18 the amount of traffic after 15 minutes was 293529.2 which eventually went higher to 320590.0 at the 45$^{th}$ minute it therefore remained constant after reaching its peak level.

### 4.5.3 Database query traffic received advanced security

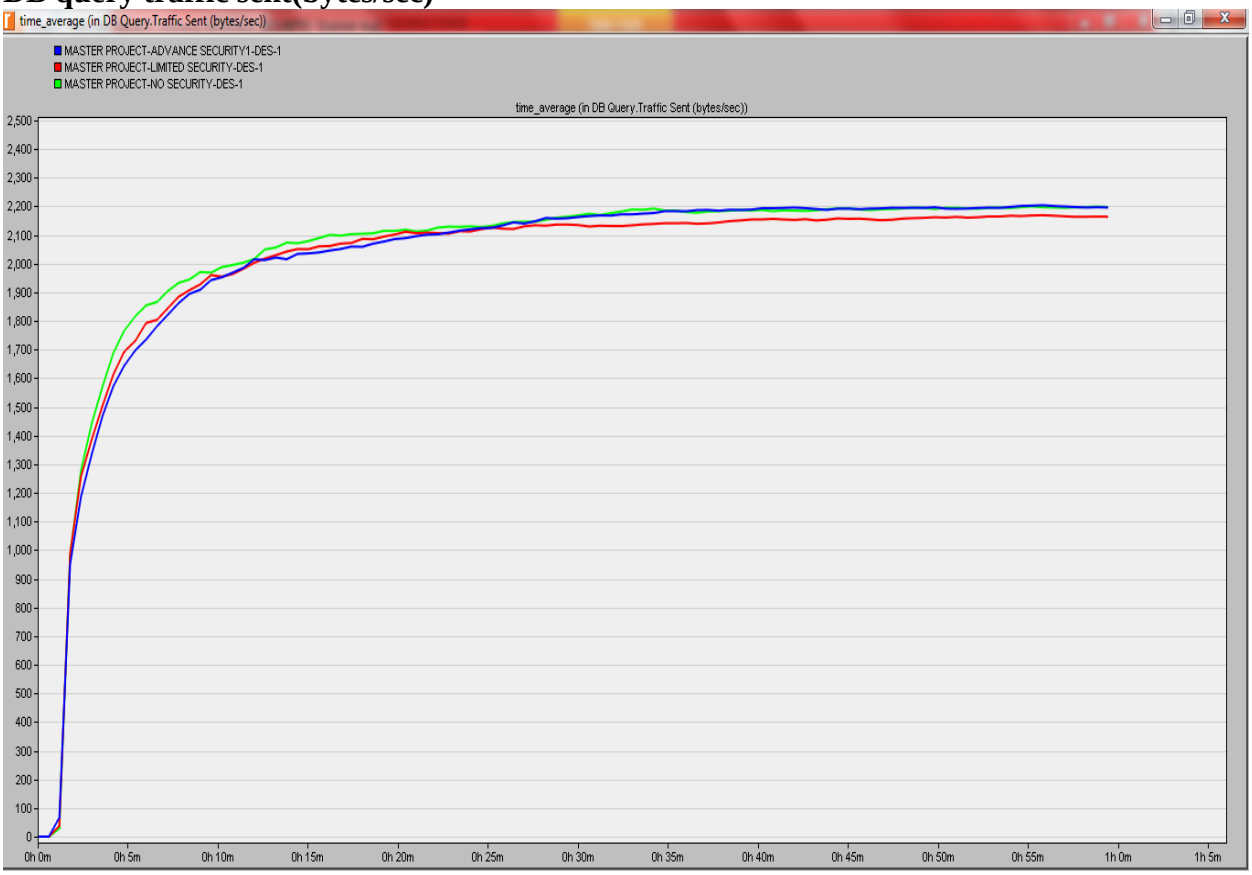
Comparing the three graphs there are no apparent changes so far as traffic received is concerned. With advanced security, there was rapid rise of traffic received within the first minute and after reaching its peak level in the 15$^{th}$ minute had gradual increase till the end of simulation.

Summary from Figure 4.3 shows there is no significant change in the amount of traffic received so far as all the three scenarios are concerned. The amount of traffic received start from the same

point and with some light deviations among scenarios but still move together to the end of simulation. The experiment depicts that there irrespective of security or no security on the network the amount of traffic flow will not change for all scenarios.

### 4.5.4 Database query traffic sent

**DB query traffic sent(bytes/sec)**




**Simulation time(mins)**

**Figure 4. 4 Database traffic sent**

Comparing the two graphs for database query traffic received and database query traffic sent, it could be concluded that when a packet size of 10mb 50mb and 100mb was passed through the network for all scenarios the amount of traffic sent is equal to the amount of traffic received. This shows that database traffic sent is directly proportional to database traffic received**.**

### 4.6 Analysis on FTP application

File transfer protocol is an application that generates lots of traffic and it also been assessed against the download and upload response time which is one key indicator in accessing network performance. It is defined as the time elapsed between sending a request and receiving the response packet. It is measured from the time a client application sends a request to the server to the time it receives a response packet.

#### 4.6.1 FTP Upload response time – No security scenario

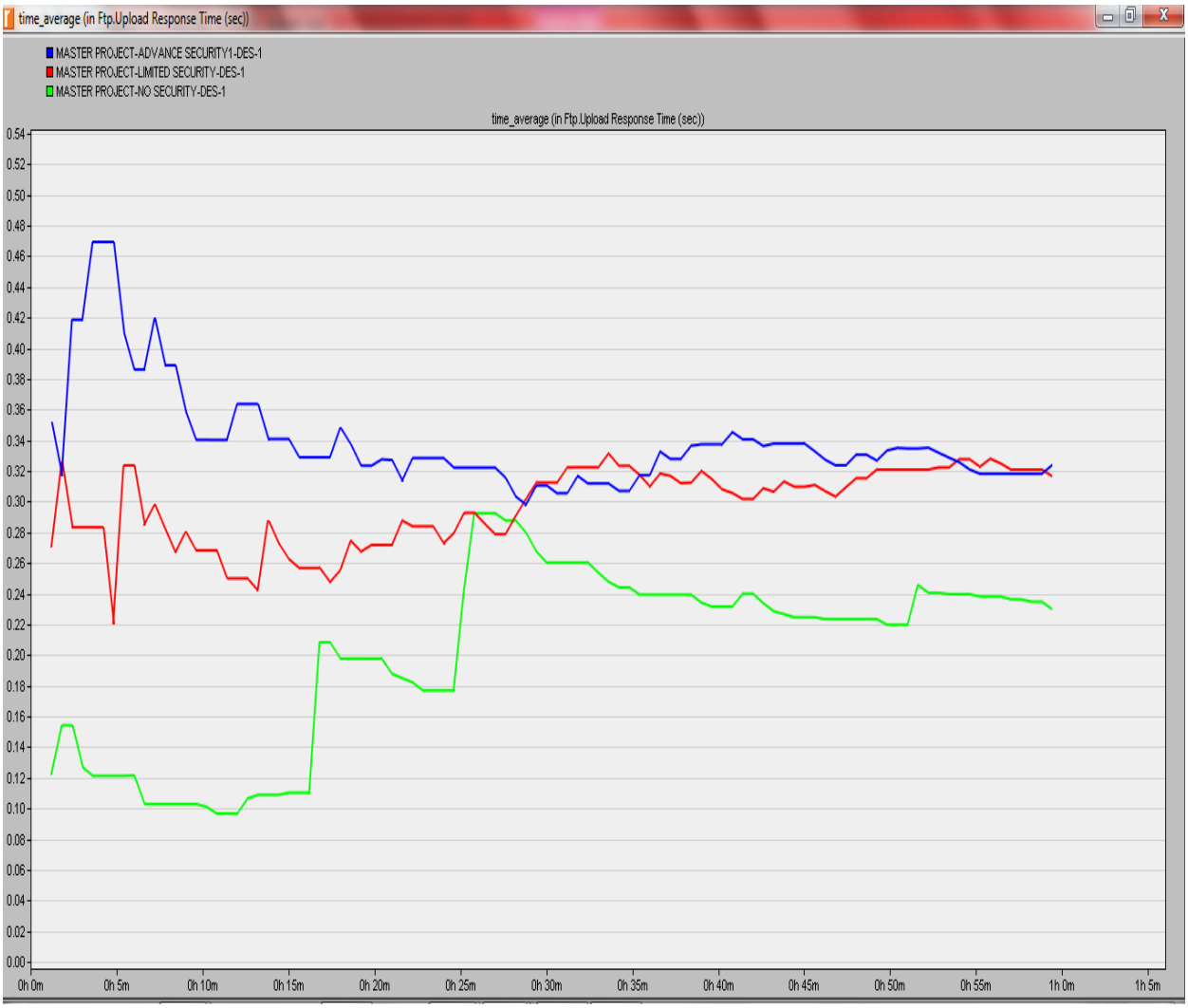



**Figure 4. 5 FTP upload response time**

The graphical overview in Figure 4.11 and the result from Tables 4.10- 4.12 shows that, there was instability in the amount of time for a user to send files to the remote server. There was fluctuating values as for the upload of files to the server. From the graph it could also be noted that after reaching its peak at the 25$^{th}$ minute which is a low value for upload there was a gradual fall. Upload response time was low means users will not experience any magnitude of delay when uploading files unto the FTP server. The scenario experienced a response time of 0.10112 after 15 minutes and afterwards the graphical pattern began to downswing thereby declining sharply and gaining some fluctuating stability between 0.22345 and 0.24001. With no security in place it could also be seen from Table 3.10 that increasing switching speed further decreases the response time.

### 4.6.2 FTP upload response time- Limited security scenario

Tables 4.10-4.12 shows the upload response time when there was packet filtering with a firewall imposed on the network and it was realized that anytime there was an increase in load, response time also tend to increase in a likewise manner.

### 4.6.3 FTP uploads response time-Advanced security

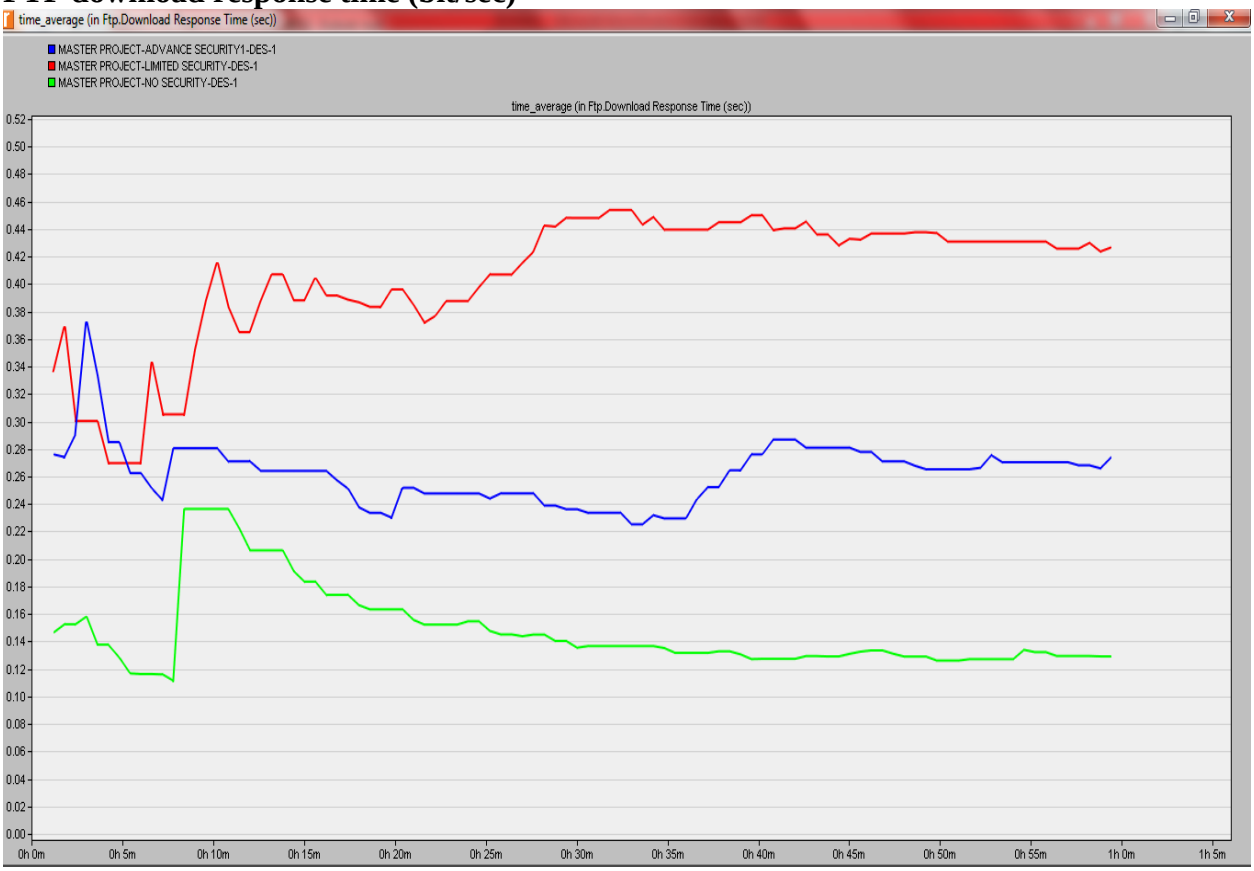
Tables 4.10 – 4.12 shows the results of advance security thus security where firewall is used for packet filtering and blocking. Having reached a niche of 0.46011 it begins to decline in a downswing manner showing some level of instability across the simulation period. But the response time went a little bit higher as compared to the other scenario, which probable indicate that for packet filtering and blocking the upload responds time will go up and decline after which it has completed. It could also be analyzed from the Table 4.10 that as the load on the network increases advance security obtains the lowest and the best response time. So it means HTTP load

from HTTP is very large and blocking some user from using HTTP applications will tend to increase the performance of the network in terms of uploading files to the FTP server.

From Figure 4.5 it could be observed that there is total instability so far as upload is concerned for all the three scenarios. The values keeps on fluctuating as file upload. This demonstrates that with or without security measures in place the time at which a file would be uploaded unto an FTP server cannot be defined. It may depend on the type of networking material and the networking environment.

### 4.6.4 FTP downloads response time- No security

**FTP download response time (bit/sec)**




**Simulation time(mins)**

**Figure 4. 6 FTP downloads response time**

Tables 4.7-4.9 shows the download response time for FTP under no security. It was realized that increasing load factor under varying switching speed increases the responds time in a direct proportionate manner. From Figure 4.16 it could be analyzed that when a load of 10mb was passed through the network, the download response time after 8 minutes reached its peak at 0.23912 after which it had a drastic fall of 0.12893 till end of simulation.

### 4.6.5 FTP downloads response time – Limited security

Following the Tables 4.7-4.9, it is seen that the download response time for limited security had a significant increase with increasing load. By the time a very high load of 100mb was imposed on the network, its value has risen greatly to between 8.063628 and 35.76077 which are higher than the other two scenarios. This is due to the fact that the firewall imposed on the network slows downloads while filtering packets with very heavy load from FTP database and HTTP (where all users of the HTTP application are using the network concurrently).

### 4.6.6 FTP downloads response time – Advanced security

Tables 4.7 -4.9 shows the results of FTP when there was advanced security (packet filtering and blocking capabilities). It remains an undeniable fact that with increasing load on the network the download response time increases. But with advance security there is a slim increment from 0.28095 and 0.524643 for 10mb and 50mb load respectively to 1.093379 for 100mb load. Considering the fact that when the load becomes very large, advance security yield good results in terms of download response there by blocking some application to enable easy download. Administrators are therefore advised to increase the performance of a network by blocking some of the applications where necessary,

However, Figure 4.6 it could be established that when a load of 10mb traversed the network advanced security lie in between limited and no security this is because advance security is

assumed to be filtering and blocking packets which is quite some good performance which records between 0.22001 and 0.240119 which is not even up to the 3 seconds response time. But for limited security is showing that graph because no application is blocked therefore all the loads are passed through network are being filtered by the firewall and it therefore raise the response time as compare to no security and advanced security.

### 4.7 Analysis on HTTP Application

HTTP application is one of the applications which generate a lot of traffic on the network. HTTP application is evaluated against the HTTP page response time. The lower the value of the response time, the faster the page opens.

### 4.7.1 HTTP page response time- No security

**HTTP page response (bits/sec)**

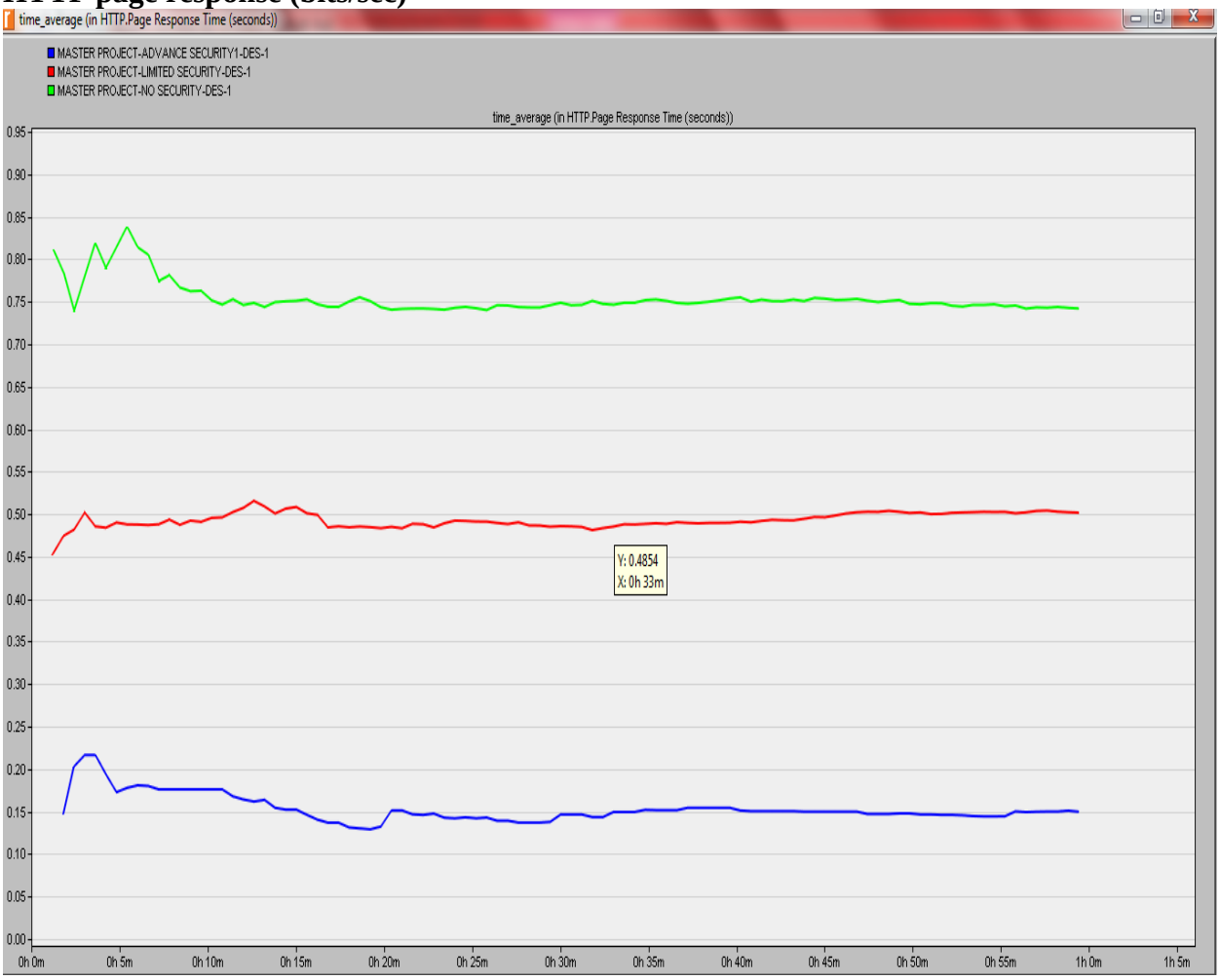



**Figure 4. 7 HTTP page response time**

The HTTP page response time is the specified time required to retrieve an entire page with all contained inline object from an HTTP server. Tables 4.4 -4.6 shows no security parametric values. The page response time was potentially higher as compared to the other two scenarios with a value of 0.84521. This means that when there is no apparent security on the network, there may be different malicious attacks on the network causing some delay on the network when a page request is made. According to Figure 4.7 the page response experienced a rapid rise within the first 5 minutes reached a peak of 0.84521 and afterward had a drastic fluctuating fall to

0.74539. It could also be realized that HTTP page response time decreases with increasing switching speed and also increases with increasing load. But with no security on the network, the page response time continues to perform poorly as against limited and advanced security with varying load on the network.

### 4.7.2 HTTP page response time-limited security

Figure 4.7 shows the HTTP page response time for all scenarios. It could be gathered that there was unstable page response time. The figures kept on fluctuating right from the within the simulation period. It was unstable, but managed to move between 0.45842 -0.52001.

### 4.7.3 HTTP page response time – advanced security

Tables 3.4 -3.6 also summarizes the HTTP page response time. From the tables advance security recorded the lowest response time with varying load and varying switching speed as against the other two scenarios. It indicates a very good performance when some of the load is blocked. Hence HTTP page responds faster when request. Blocking some applications optimizes the performance of a network when a web page is requested.

Comparably, Figure 4.7 it could be clearly observed that the response time when HTTP page is queried remains steadily with little or no fluctuations from start to end of the simulation. However, advance security scenario has the lowest values for page response as compared to limited and no security scenario. But the lower the response times the better. Therefore advance security shows a response time between 0.149915 - 0.152309. There is a clear indication that when an application like HTTP which creates heavy traffic is blocked it causes other ones respond faster.

# CHAPTER FIVE

# FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

## 5.1 Findings

The experiment performed was to measure and to test for some key performances of the network. The performances were also based on the application that was deployed onto the network for analysis.

The simulation experiment was used to measure the following.

i. the performance of applications when no protection is on a network
ii. the performance of applications when the protection is limited on a network
iii. the performance of applications when there is maximum protection on a network

Simulation results in Figure 4.1 depict the Ethernet delay on the network. When there is advanced security (firewall with blocking) on the network using the OSPF routing protocol, the Ethernet delay is slightly higher and that of limited and no security is lower.

The delay started form different amplitude but became very stable at an average value. The three network scenarios almost experienced the same delay across board.

Similarly Figure 4.2 depicts the database query response time and it is evident no security scenario has the worse response time advanced security scenario showing the best performance in terms of response.

At the same time Figure 4.5 shows FTP uploads response time. No security scenario had the best performance in terms of ftp uploads as compared to other two scenarios. It is also clear from

Figure 4.5 that the upload response times is very close and intersect at some point within simulation time.

Figure 4.6 also shows a FTP downloads response time. It shows a clear distinction between all the three scenarios as simulation progresses. Hence they are not closer as compared to the upload response time and do not intersect as well. The no security scenario still has the best response time with limited security showing a worst response time.

It is also evident that FTP uploads and downloads response times are very close and low for FTP applications. Page response time was evaluated for HTTP applications. Figure 4.7 shows page response time for http application and it could be observed that response time was lower and better for advance security scenario when HTTP traffic was blocked for some users.

### 5.2 Conclusion

In todays' computing, companies are striving to optimize their level of protection day in and out by installing firewall systems onto their network. As load increases the performance of the network degrades. But user experience must not be affected when there is change in security. Customer service must be a key factor in every organization and must be appreciated in that customers do not wait hours before being served. Security methods like the use of firewall may cause poor performance in a network depending on the application being used. Computer network was modeled to no security, limited security and advanced security and the network was simulated with deep closeness on applications performances.

### 5.3 Recommendation

From the experiment it could be clearly observed that network security with or without firewall security traffic still flow through the network at varying speed and load. Also application

performance depends on the types of security protection conferred on the network. The flow of network traffic is also not stable with firewall security therefore company's turning to use firewall security should be expecting some instability in the flow of network traffic. However it is was observed that http applications has heavy load and creates lots of congestion on the network, company's experiencing network congestion can improve upon it by disallowing http traffic through the network or may improve the switching speed of their LAN.

## REFERENCES


Avolio, F. and Ranum, M., (1996), "A Network Perimeter with Secure External Access," Proceedings of the ISOC NDSS Symposium Available at http://www.avolio.com/papers /isoc.html (Retrieved: 6 March 2014)

Avolio F. (1999), Firewall and internet security. *The internet protocol journal*, Vol2, No.2

Behringer M. (2011), Network complexity and how to deal with it Available at http://labs-ripe.net/members/mbehring/network-complexity-and-how-to-deal-with-it

Bhaiji Y. (2008), "Network Security Technologies and Solution", Cisco press, Indianapolis

Boom P. & Boom A. (1998) "Securing network applications with SESAME" Available at http://www.linuxjourna l.com/article/2453 (Retrieved: 11 November, 2013)

Bui S., Enyeart M. & Jenghuei L. (2003) "Issues in computer forensics" Available at http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf (Retrieved:10 June, 2014)

Castelli M., (2002), Network Performance Handbook, Cisco press, Indianapolis

Canavan J.E (2001), Fundamentals of network security, Artech House Inc, Norwood.

Chapman, D. B. and Zwicky, E., (1995), Building Internet Firewalls, O'Reilly and Associates

Cheswick R.W & Bellovin S.M & Rubin A.D (2003) Firewall and Internet security, 2nd Edition. Addison-Wesley.

Cisco Unified Communications Manager Administration Guide (2009), Cisco Systems Inc., San Jose, USA

Computer Services Group (2016), "Why is network security important". *Evolution of networks Part I*, Available at http://www.computer-services.com.au/services /network-security (Retrieved: 1 January, 2016)

Damien M. (2002 "), SSH tips, tricks & protocol tutorial" Retrieved: 14th May,2014)

Danscourses(2013), Network security overview. Background on network security Available at www.danscourses.com(Retrieved: 1 June 2013)

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases.Hoboken NJ: John Wiley & Sons.

Fosnock C.(2005), "Computer worms: Past, Present and Future" Available at https://vxheaven.org/lib/pdf/Computer%20Worms:%20Past,%20Present,%20and%20Future.pdf (Retrieved: 4th May 2014)

El Gamal A., Mammen J., Prabhakar B., & Shah D. (2004), Optimal Throughput-Delay Scaling in Wireless Networks – Part II: *The Fluid Model*, Available at http://www.stanford.edu/˜jmammen/papers/it-TDpkt.pdf. ( Retrieved: 15th November, 2013)

Fuzner M. (2013), Graphical Network Simulator version1 Available at http://www.csd.uoc.gr /~hy435/ material/ GNS3-0.5-tutorial.pdf (Retrieved: 9 January,2015)

Garfinkel S. & Spafford G.(1996), "Practical Unix and Internet Security",2nd Edition, O'Reilly & Associates Inc, CA

Hancock J.(2004), Jitter- Understanding it, measuring it, eliminating it. *Jitter fundamentals Part 1*, pp. 44, Summit Technical Media LLC

Highlands J.H (1997), A history of computer viruses- The famous "trio",vol.16, No.5, Ppg. 416-429

Kaeo M.(2003) "Designing network security", 2nd edition, cisco press, Indianapolis

King T.(2002), Packet sniffing in a switched environment. *Nework security resources* Available at http://sans.org/network-security(Retrieved: 10 August, 2014)

Lateef A.B, Sudan V & Kirat P.S (2013) "Interior Gateway Protocols", vol. 4 Surya World, Punjab, India.

Lewis M. (2006), Comparing, Designing and Deploying VPNs, Cisco press, Indianapolis USA

Mathivilasini S. & Srivatsa S.K (2015), A study on the benefits of network security in wireless sensor network issues. *International Journal of Applied Environment Science*, vol.10, No.1, pp 41-46

Mohammed A.B, Idris N.B & Bharanidharan S. (2012), "A brief introduction to intrusion detection system". *Trends in Intelligent Robotics, Automation, and Manufacturing*, pp.263-271

Natin A.N, Kurundkar G.D, Khamitkar S.D & Kalyankar D.V (2009), "A Roadmap to Network Security" *Penetration testing* ,vol. 1 pp.187-190

Partsenidis C. (2013), Disadvantages of early VPN. *A History of VPN* Available at http://search enterprisewan.techtarget.com/tip/A-history-of-VPN-Disadvantages-of-early-virtual-private-networks (Retrieved: 13 June 2014)

Radware solutions (2012), History of network security. *Evolution of networks* Available at http://www.radware.com/Resources/network_security_history.aspx(Retrieved:8 May, 2014)

Reeshil N. (2011), Layers of OSI Model and TCP/IP model. *Network architecture* Available at: http://ayurveda.hubpages.com /hub/OSI-model-and-TCPIP-model (Retrieved: 17 March, 2014)

Santos O, (2007) "End to end network security: Defense-in-depth", cisco press, Indianapolis

Scott C., Wolfe P. & Mike Erwin,(1999). Virtual Private Networks, Second Edition, O'Reilly

Steinemann M.A, Spreng T, Bachmayer A, Torsten B. Graf C. & Guggisberg M.(2003), "Authentication and Authorization Infrastructure: Portal Architecture and Prototype Implementation", vol. 1, Available at http://aai-portal.sourceforge.net/doc/aai-portal-v1.0.pdf (Retrieved: 30 September2013)

Wang J. (2015), The VIRLBOOK: A guide to CISCO'S virtual internet routing lab Available at www.firewall.cx (Retrieved: 10 March 2015)

Watson R.T (2007), Information Systems, Global Text Project

Whitman M.E & Mattord H.J (2012), Principles of Information Security, 4th edition, Cengage Learning, Boston

Zester L.(2010), “How to respond to an unexpected security incident” Available at http://zeltser.com/presentations/unexpected-incident-response.pdf (Retrieved: 5 June, 2014)