ENSC 427: COMMUNICATION NETWORKS

Spring 2012

Final Project Report

Evaluating the Performance of Security Mechanisms in Networks over the Internet

Web Address: http://www.sfu.ca/~msa102

Soleimani-Nouri, Maxim 301103660 msa102@sfu.ca
Cheng, Andy 301090416 alc21@sfu.ca
Mehdizadeh, Saman 301092517 sas20@sfu.ca

Date: April 15, 2012

Simon Fraser University

Team #2

Abstract

Today, security is a critical topic of discussion with the rapid growth of Internet and communication networks. Currently, a lot of services such as Hypertext Transfer Protocol (HTTP), Electronic mail (Email), and File Transfer Protocol (FTP) are provided and made available to clients with Internet access anywhere in the world. These networks offering the mentioned services are usually web servers located in different regions giving access to clients through routers. However, routers do not restrict access and allow all different kinds of traffic through. This could cause problems as some services or shared resources may be confidential and not viewable to general public. Installing firewalls across networks to restrict access depending on various configurations can solve such problems. Firewall is simply a router positioned in between two or more networks to filter unwanted traffic and packets that flow through it. Virtual Private Networks (VPNs) can also provide a method of controlled connectivity between two or more nodes on the Internet for clients to have full or limited access and authority over the provided services and resources online. This project will analyze the use of Firewall and VPN along with different types of intrusions using OPNET 16.0. Different scenarios along with simulation and results will be discussed in this project. As will be seen later in the results and discussion section, introduction of firewalls and VPNs will help secure networks and block unwanted traffic and only allow access to authorized users. Nevertheless, the use of these security mechanisms will introduce a slight delay in data transmission and an increase in the number of hops will be observed. This could be an unwanted situation under different circumstances such as time-sensitive communication networks.

Table of Contents

Table of Figures

1.0 Introduction

1.1 Scope

The scope of this project will encompass a thorough analysis of a standard network topology utilizing two main methods of security mechanisms: Firewalls and Virtual Private Networks (VPNs). Three scenarios will be simulated, with each subsequent one building on the previous:

- **Default**: 3 workstations and server connected to Internet through individual routers
- **Firewall**: replace server router with firewall
- **Firewall & VPN**: place a router between server router and server

Various statistics including node traffic, delay, and jitter will be collected in the simulation and will be used to investigate each of the scenarios in question.

1.2 Motivation

The motivation behind this topic begins with the creation of the Internet. The service did not really take off until 1989 -2003 with the introduction of the World Wide Web and graphical browsers. Now, the Internet has become the largest, most complex network where data is continuously exchanged from client to client around the globe. The world has entered an age where anyone can access the Internet. At the same time, because people have become so accustomed to the ease and convenience the Internet offers such as banking services and data storage that very same entities known as “thieves” have manifested themselves on the web. The existences of these malicious users who try to steal digital information and disrupt services have led to the advent of Internet security [1].

While there are many ways to protect computers as well as privacy and data from being misused, we will strictly look at only firewalls and VPNs. The firewall is essentially an “impenetrable” wall preventing all forms of access to the protected network unless specified by the administrator. VPNs on the other hand will allow a user to connect to the services provided by the protected network even with the presence of a firewall [2]. Of course, to make sure the session is kept private, all packets sent between network and users are encrypted.

For a starting point, we will create some simple scenarios to compare the relative effects of our proposed network defenses against basic access attacks. For example, we first model the topology to include a server and three users each with their respective routers and no firewalls, all connected to the Internet Protocol cloud. Any query the users send to the database should be returned, so the received traffic for the users should match the amount of data they are requesting. In another scenario, we replace the server's router with

a firewall and observe the same statistics. However, with the firewall properly setup, the users who are denied access to the database should not be getting any receiving traffic. This is one of the methods of evaluation we will use to analyze the effectiveness of network security methods against outside attacks.

2.0 Related Works

When setting up a network, especially for corporations who rely upon services offered by their network, one of the main concerns is how to setup a reliable, secure network. Of course, some of the most common and effective ways of doing so are to use firewalls and VPNs as the topic of this paper attempts to evaluate. However, there are other elements and techniques which can be employed. This is why the subject of security has been much focused upon in the Internet conferences community.

One method to combat high traffic is to simply expand the hardware; the more backend servers you have, the more traffic the servers can handle in total. Backend servers are basically the servers that are "hidden" behind another server who is configured as a reverse-proxy. The reverse-proxy server handles the requests while the backend servers the ones who actually process the requests [3]. Outsiders to the network will not be able to see the servers. This implementation is shown in Figure 1a below.

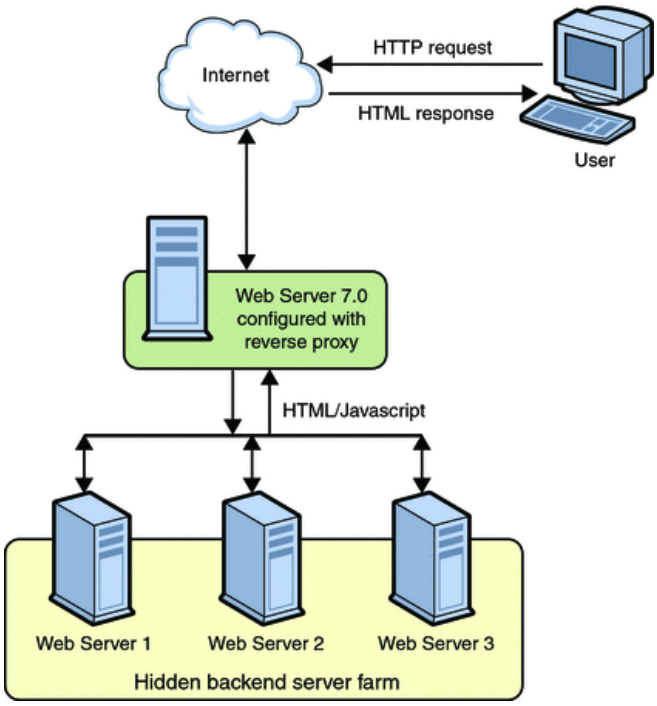

Figure 1a: Reverse-Proxy with Backend Servers

However, it becomes a challenge to evenly distribute the amount of requests per server such that no server will be overloaded with requests while the others are unused. The use of a load balancer can help distribute

the amount of load among the backend servers to combat this issue, as supported by the simulations of Sapna and Sharma [4].

Another point of interest is the differences between wired and wireless networks. Generally, wired networks tend to offer better performance and lower latency as opposed to wireless networks. What this paper attempts to show is the performance of firewalls and VPNs in a wired network. There is no doubt that the inclusion of such security devices will amplify some latency issues in a wireless scenario. The conclusions made here can be used as a comparison and supplement perhaps to the work of Y.P. Kosta et al who further explore the effects of firewalls and VPNs using a wireless setup [5].

3.0 Firewall

The firewall provides the most basic protection against unwanted, unauthorized access to a network or particular service. In essence there are two kinds of firewalls, software and hardware. Hardware firewalls mainly deal with incoming packets; they regulate what kind traffic is allowed to enter. Software firewalls on the other hand are installed directly on the operating system, and can prevent applications from sending or receiving traffic [6].

In order to provide a more robust security, hardware and software firewalls are usually used in conjunction, especially in large corporations where a lot of proprietary digital information is stored. There are three main types of firewalls [7][8]:

1. Packet filtering
2. Stateful inspection
3. Application

Each of which, providing certain improvements over another. The following sections will discuss the details of each type of firewall and look at the advantages and disadvantages.

3.1 Packet Filtering Firewalls

The simplest and earliest firewall deployed was the packet filter. Its function is simply to look at the source and destination information from the header. It then compares that information to a set of rules defined by the user or administrator to determine whether the packet is legitimate traffic. If the packet is not, it is simply dropped.

3.2 Stateful Inspection Firewalls

Stateful inspection firewalls emerged during 1989-1990, and is technically an upgrade to the packet filter. In addition to inspecting header information, it can also keep track of the session information [7][8]. Essentially it keeps track of all connections that are currently in use by the network and determines whether the payload contains the appropriate data. For example, if the firewall knows that a Hypertext Transfer Protocol (HTTP) connection is currently in use, then any packet that attempts to enter must also contain legitimate HTTP data. If it doesn't, the packet is also dropped. Figure 1b below summarizes the idea of a stateful packet inspection firewall into five steps.

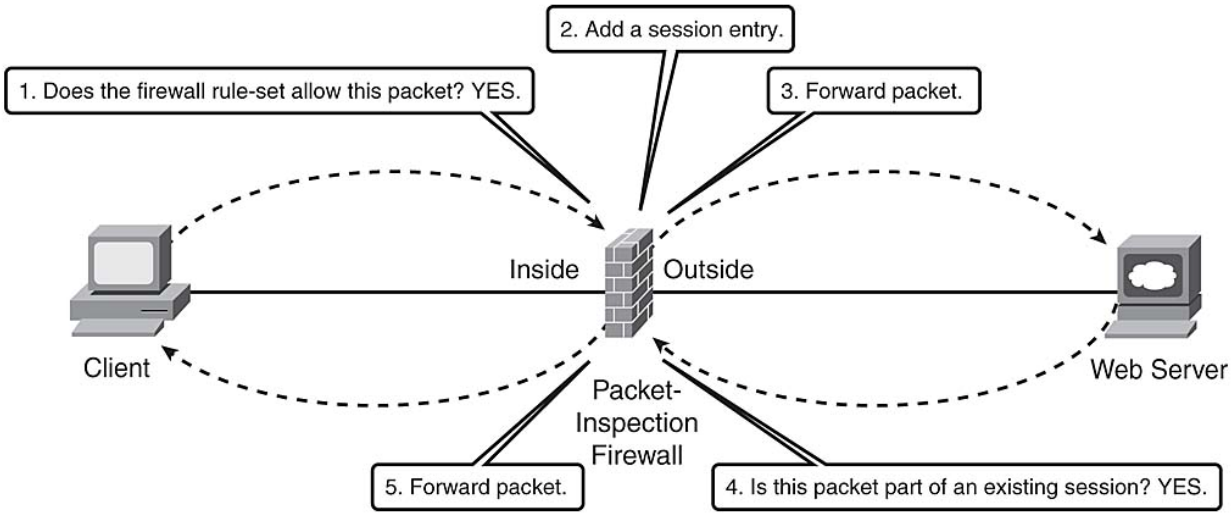

Figure 1b: Stateful Inspection Firewall

3.3 Application Firewalls

Application firewalls can be classified under software firewalls in that they control the bi-directional flow of traffic. What this means is that any packet entering and leaving the network will be inspected against a set of rules setup by the administrator. Rather than looking at each individual packet, the application firewall controls all input, output and access up to and including the application layer of the OSI [7][8]. Application firewalls can be further broken down into two subtypes: network-based and host-based. Host-based firewalls refer to software installed on the host computer or server, such as WinGate or WinRoute for machines running Windows OS. On the other hand, network-based application firewalls, otherwise known as a proxy-based or reverse-proxy firewall are usually installed on a standalone network device. The concept of a proxy is that it acts as a medium between the host and Internet. All packets requested by the host must first be delivered to the proxy. After it determines the data is safe, it then forwards the requested data through the protected network to the host. Figure 2 below illustrates the idea of a network based application firewall.

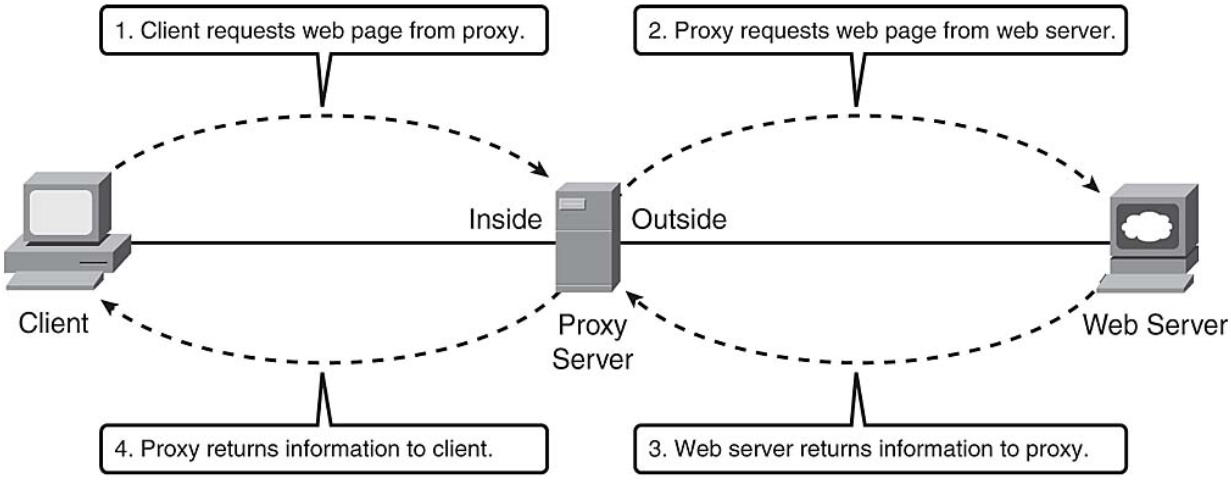

Figure 2: Network-based Application Firewall

4.0 Virtual Private Networks (VPNs)

VPNs provide a secure method of data transmission on non-secure networks using the tunneling concept described below. VPNs do not require physical connection and any user with access to Internet can establish a VPN connection under the right circumstances. For this reason, VPNs are widely used in different network infrastructures. There are generally two types of VPNs: remote access and site-to-site VPNs. Site-to-site VPNs refer to users accessing the network in a fixed location. However, the main purpose of using VPNs is due to its ability of providing a secure and flexible way for remote users to access data on secure servers regardless of the firewall protecting the network. Hence the main emphasis of VPNs are placed on remote access for employees from different regions/branches or off-site users trying to access data and information on the company server which is being protected by a firewall via Internet.

4.1 Tunneling

Tunneling is the concept of transferring data securely between two networks or nodes. A tunnel is the logical path between two nodes consisting of transmitters and receivers. First, the data is broken down into smaller packets or frames. Next, these packets or frames are encapsulated at the source and additional tunneling encryption layer is added before transmission of data. After the completion of data transfer, the packets and frames are encapsulated and decrypted at the destination and directed towards the correct node located in a given network [2].

4.2 Types of Tunneling

There are two types of tunneling: voluntary and compulsory. Voluntary is when a client initiates connection with a VPN server creating a secure tunnel for data transfer between the two nodes. Compulsory tunneling is the connection created between two VPN servers or two VPN routers [2]. Connections can be created through Local Area Networks (LANs), which require physical connection, or through the Internet targeted towards remote users for ease of access.

4.3 Types of VPNs

There are two types of VPN deployment in a network being protected by a firewall. The first type consists of VPN server which is placed in front of the firewall. This architecture requires additional packet filters to allow only VPN traffic between the Internet and VPN server interface. This method is less common as it "prevents the sharing of File Transfer Protocol (FTP) or web intranet resources with non-VPN Internet users" [8]. The second type is the deployment of the VPN server behind the firewall. This configuration is more common and is typically used in secured networks with firewalls. Moreover, the firewall requires input and output filters to allow passing of tunneled data to the VPN server. The second configuration will be used in this project for implementation/simulation purposes. The typical setup of this type is shown in Figure 3.

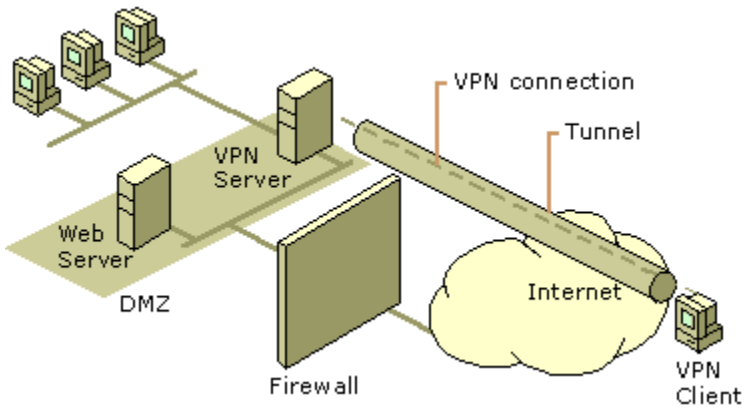

Figure 3: VPN server behind firewall

5.0 Simulation

In order to simulate the proposed implementations, the topology must first be created. The following subsections show the topology of the respective scenario in OPNET Modeler 16.0. Note that the default scenario is simply the same as the firewall scenario, except that a router replaces the firewall.

In order to generate traffic, the users must be able to run applications. First, an Application Configuration node is created. In attributes, the value of “Applications Definitions” was set “default”. This provides a basic set of applications predefined by OPNET. A second node, Profile Configuration, was created. This is used to create a profile of sorts, which are basically a collection of applications. In all simulations, a user profile was created specifically to use HTTP (Light) and Database (Light) applications.

In all scenarios, the links used are PPP DS1, which has a maximum bandwidth of 1.544Mbps. The simulation time was set to one hour, and the average time it took to complete the simulation was under one second. Due to hardware limitations in the laboratory, resource intensive applications such as video, voice, and any “heavy” variant were avoided to reduce the simulation time. Needless to say, it has been tested that the aforementioned applications cause an exponential increase in the time to complete the simulation from less than a second to onwards of ten to twenty minutes.

5.1 Default Scenario

In the default scenario presented by Figure 4, three workstations are connected through individual routers to the Internet cloud (IP).

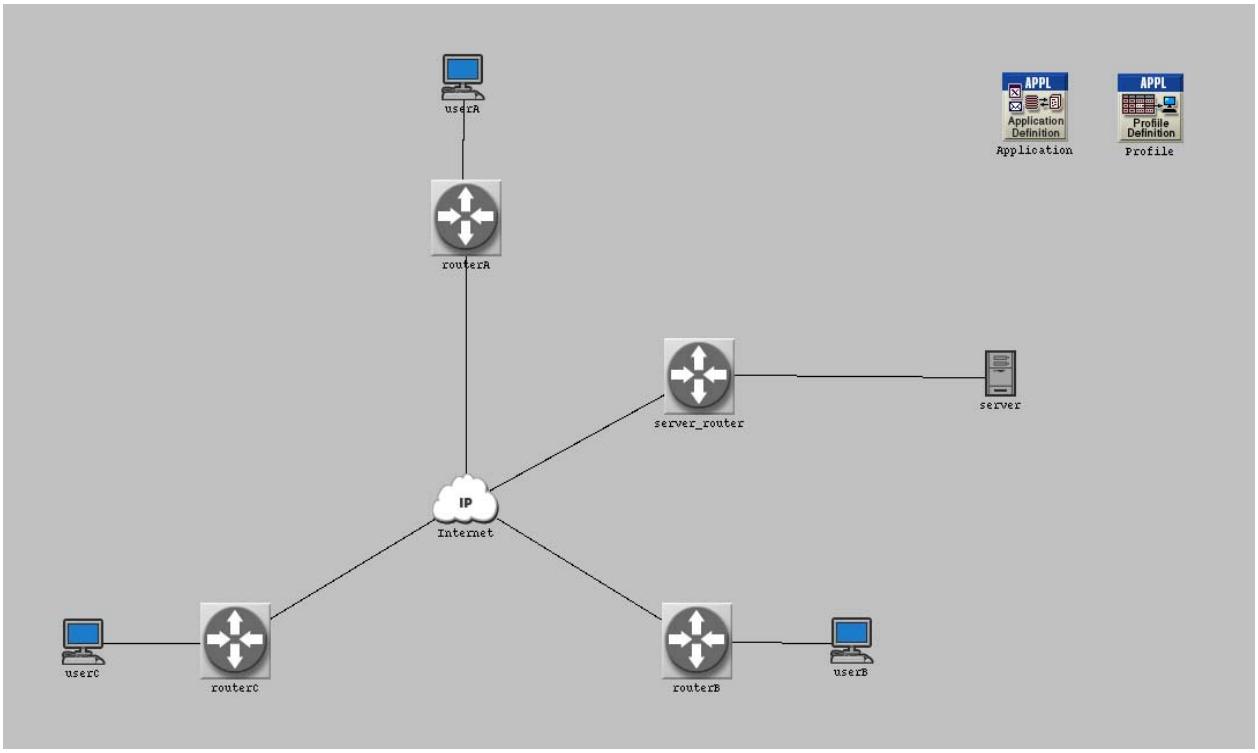

Figure 4: Default scenario topology

5.2 Firewall Scenario

The firewall scenario replaces the “server_router” model with a firewall model named as “firewall” in Figure 5 below. The purpose of the firewall in this project is to block all incoming and outgoing database application traffic. It will not limit the use of HTTP, and will act as a proxy for users and server. To configure the firewall model to block the database applications, the value for “Proxy server deployed” must be set to “no” under row 1 in the firewall attributes. By default, all other applications are set to “yes”. This procedure is shown in Figure 6.

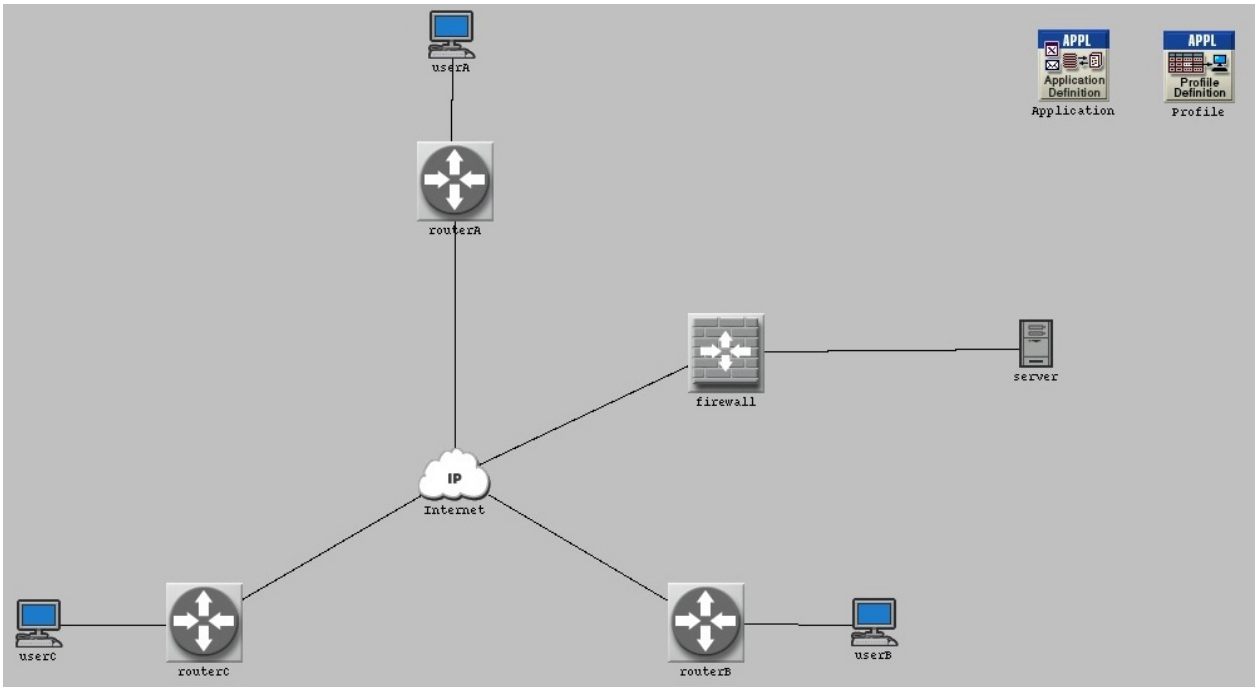

Figure 5: Firewall scenario topology

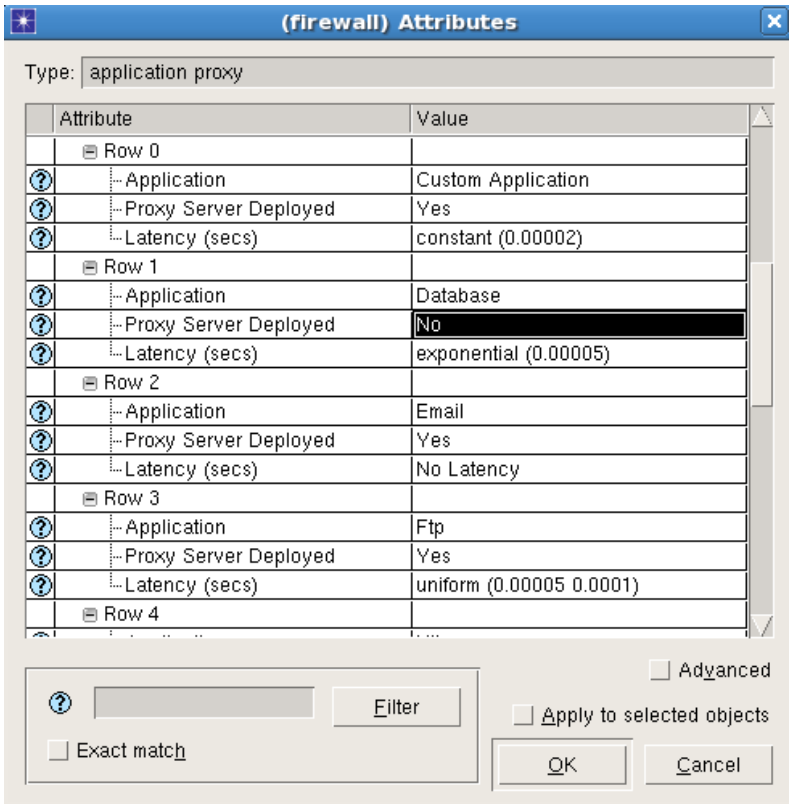

Figure 6: Firewall attributes

5.3 Firewall and VPN Scenario

The third and final scenario will introduce the use of a “VPN config” node and another router between the firewall and server as seen in Figure 7. The new router introduced, named “VPN_router” will create a tunnel between userA and server such that userA can bypass the firewall’s database restrictions. To setup the VPN, the “VPN config” node must be configured exactly as shown in Figure 8.

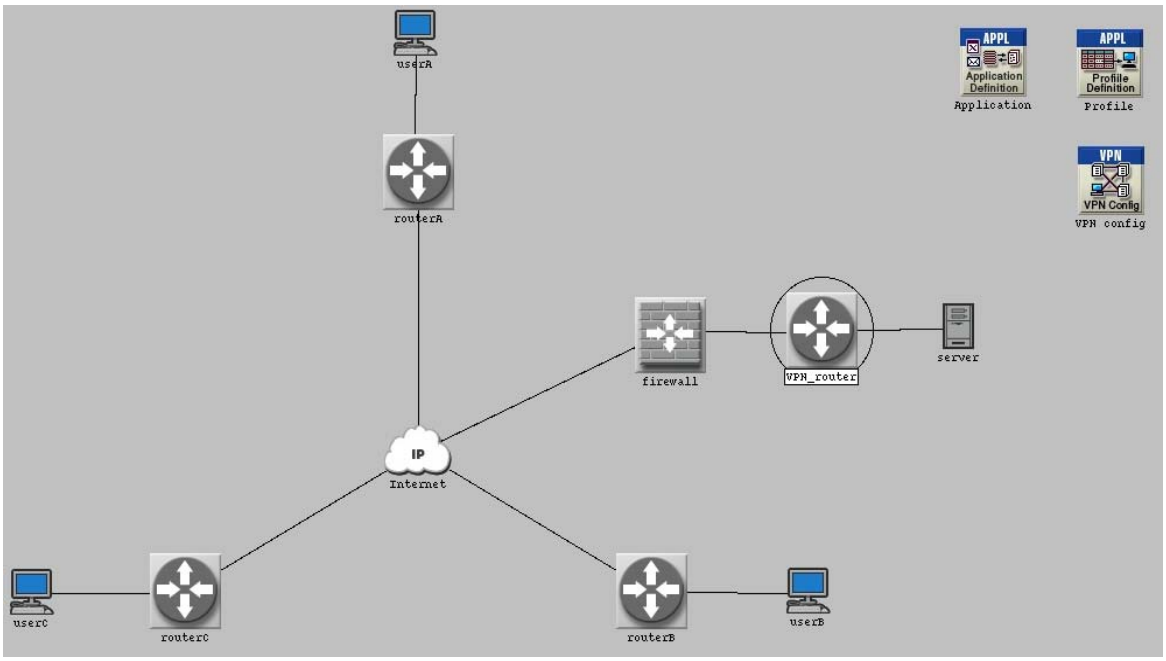

Figure 7: Firewall and VPN scenario

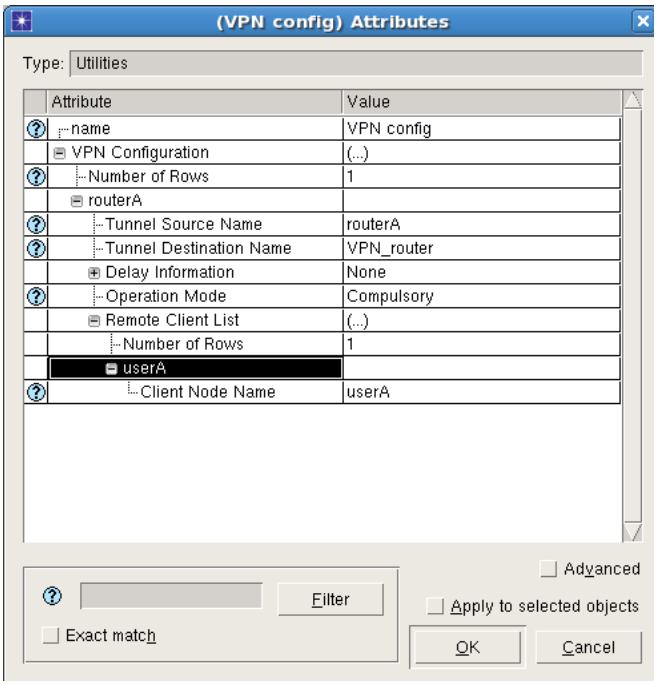

Figure 8: VPN attributes

6.0 Results and Discussion

To analyze the performance of the simulated scenarios, several statistics were recorded during simulation. Table 1 shows all individual and global statistics taken.

Table 1: Simulation Statistics

Individual (userA,userB, userC)	Global
Incoming Database Traffic (bytes/sec)	Database Query Response Time (sec)
Incoming HTTP Traffic (bytes/sec)	HTTP Web Page Response Time (sec)
End to End delay (sec)	Number of Hops
Jitter (sec)	Number of Packets Dropped (packets/sec)

6.1 Comparison of Incoming Traffic

To determine whether the implementation of the firewalls and VPN were successful, the time average of application traffic received is observed. For userA, no traffic is seen in the firewall scenario. This is shown in Figure 9. This is correct because userA should only have access in the default and VPN scenario (since it is tunneled). UserB on the other hand receives traffic only in the case of the default scenario (Figure 10), meaning the firewall was working properly and the VPN only allowed access to userA. For the case of HTTP traffic, no rule was placed on the firewall to restrict the application in any way. As seen in Figure 11 and Figure 12, both userA and userB had a consistent flow of incoming HTTP traffic in all scenarios.

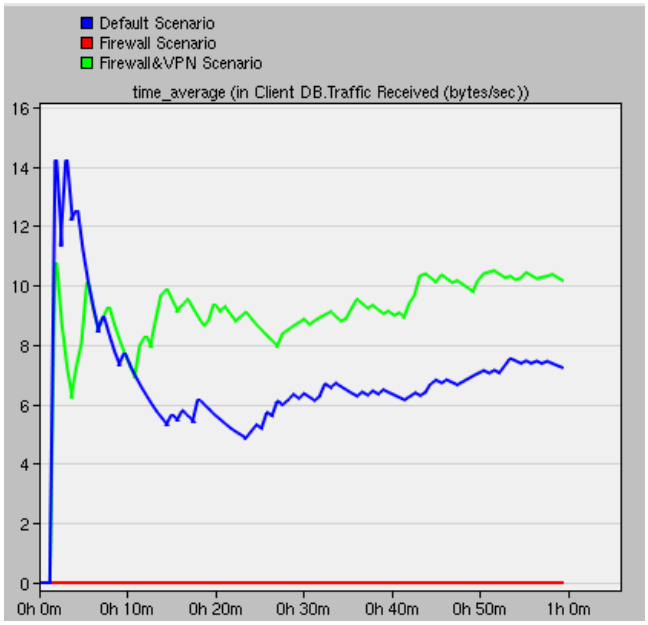

Figure 9: userA Database traffic in Default scenario

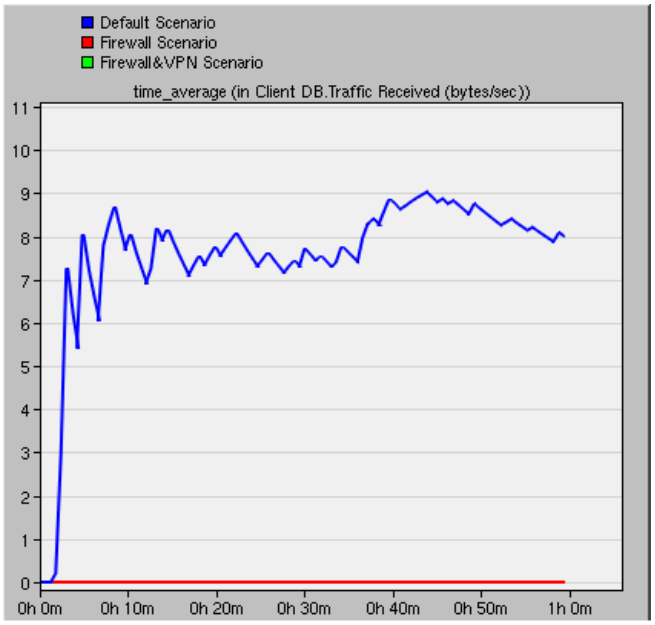

Figure 10: userB Database traffic in all three scenarios

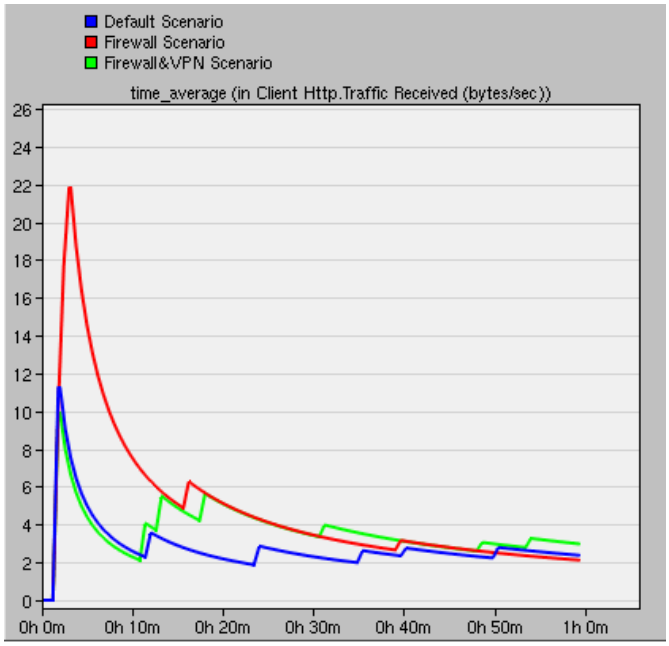

Figure 11: userA HTTP traffic in all three scenarios

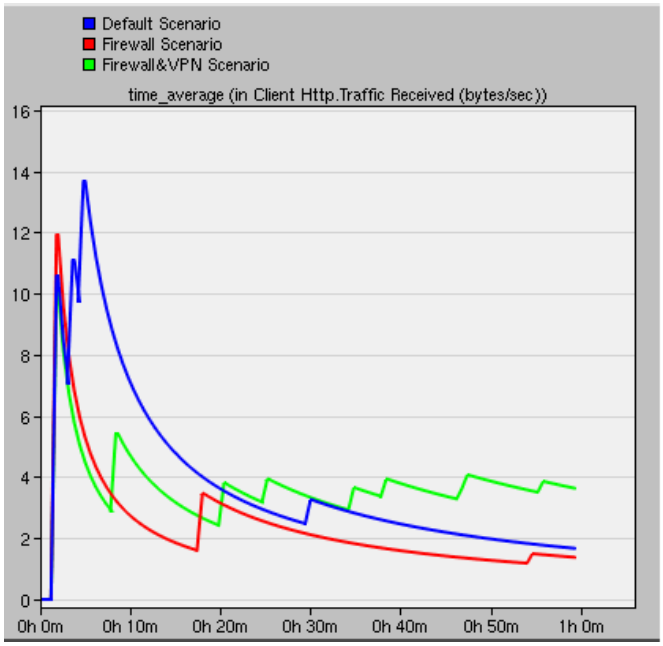

Figure 12: userB HTTP traffic in all three scenarios

6.2 End-to-end Packet Delay

End-to-end delay is the amount of time it takes for a single packet to travel from the source to destination through the network. It can be observed from userA shown in Figure 13, that the use of a VPN introduced a higher average delay. UserB on the other hand saw more delay in the default scenario presented by Figure 14. This is because in the default scenario, there was more traffic as no firewall was blocking any application.

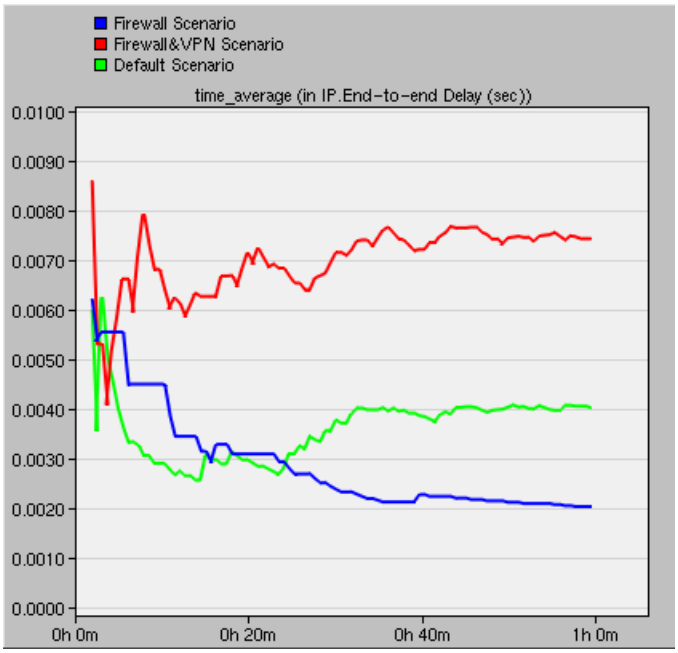

Figure 13: userA end-to-end packet delay

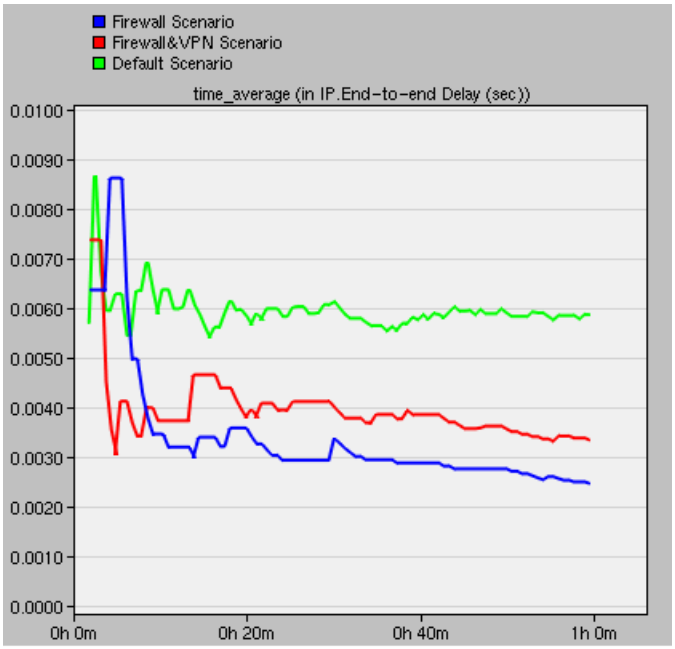

Figure 14: userB end-to-end packet delay

6.3 Variation in End-to-end Delay (Jitter)

When a user is requesting a service over the Internet, he or she is expecting a smooth transfer or constant bitrate. Why is this important? Consider an application such as video where it is crucial to have fluid animation. Variation in the end-to-end packet delay is what causes the stuttering and inconsistent display of images that appear in a video, and thus it is desirable to minimize jitter. From the userA jitter graph represented by Figure 15, it is clear that the use of a firewall in conjunction with a VPN causes an increase in variation almost on the order of two. It may not seem like a lot, but this is because the simulation is only concerned with light traffic. The introduction of heavier traffic will definitely amplify the effects of this delay variation seen in VPNs.

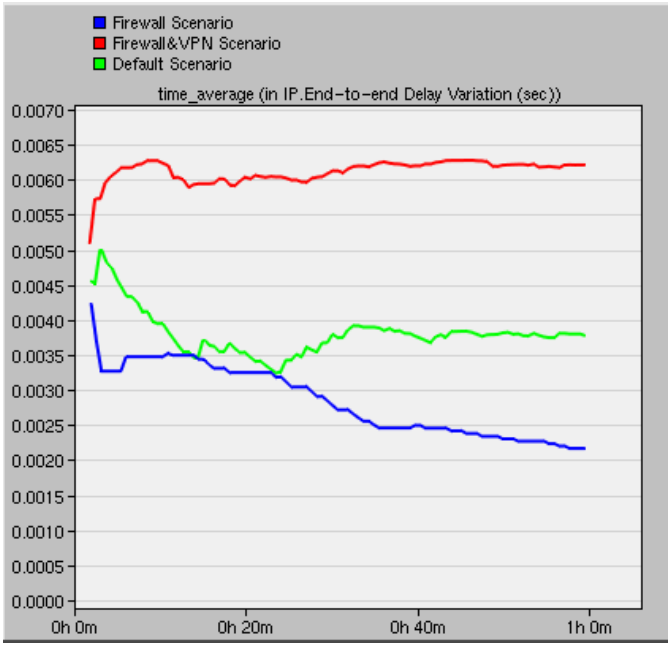

Figure 15: userA traffic jitter (increased)

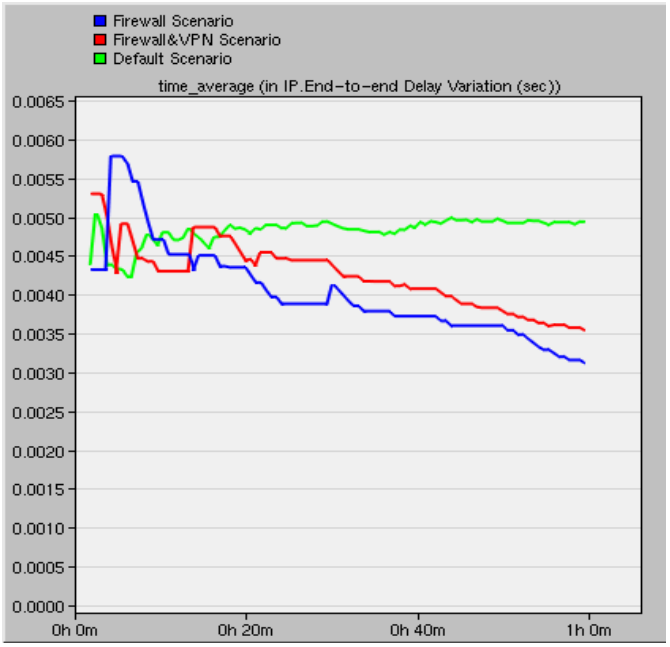

Figure 16: userB traffic jitter (normal)

6.4 Global Application Response Time

To get a sense of the response time over all applications and scenarios as a time-average, OPNET was configured to collect the global application response time. Figure 17 shows that the average response time for database applications in the Firewall scenario is slightly longer than that of the default scenario. Similarly, the HTTP also shows that the use of VPN introduces roughly 23.33% more delay than that of the other two scenarios. This is shown in Figure 18.

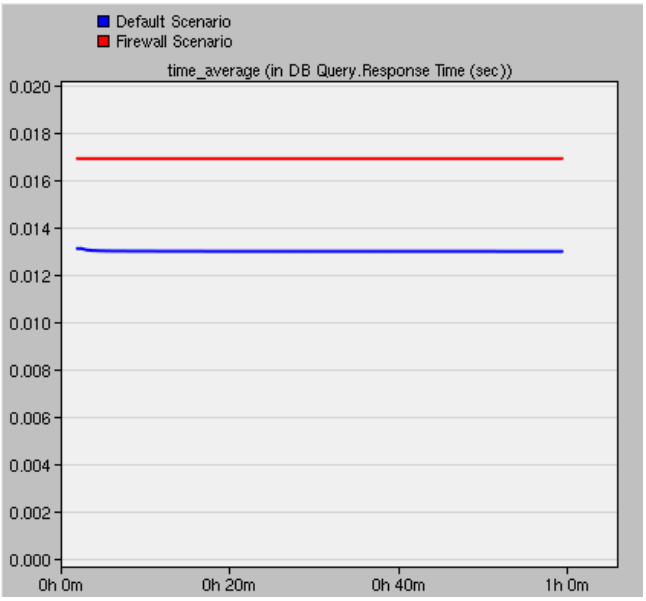

Figure 17: Database average response time

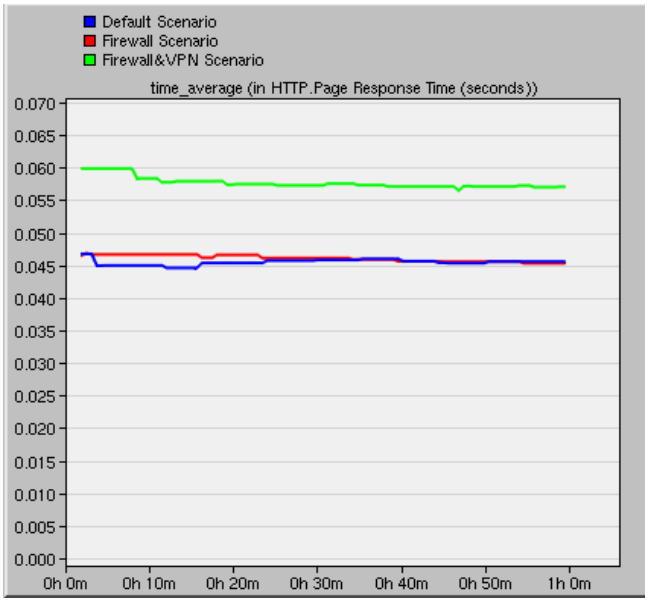

Figure 18: HTTP average response time

6.5 Number of Packets Dropped

Although looking at the traffic received for individual users should be enough to see whether the firewall was working, it is not sufficient. Firewalls will drop any packet that is blacklisted and therefore provides concrete proof that it is indeed preventing database application access. From Figure 19, it can be concluded that packets are being dropped in the firewall and VPN scenarios. The VPN scenario should have less packet loss because userA is being tunneled to the VPN_router, thereby allowing the database application packets to pass through, which translates to less packets lost overall.

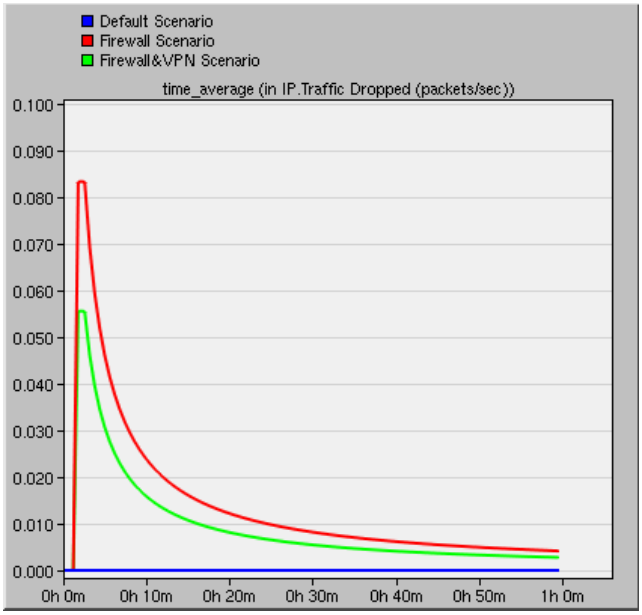

Figure 19: Traffic dropped

6.6 Number of Hops

Here, Figure 20 shows the number of hops as a time average in all scenarios. A hop is the distance between two physical network devices. Taking the firewall scenario as an example, a packet sent from userA will have to travel to routerA, then to IP cloud, then to the firewall, and finally to the server making a total of four hops. It is interesting to note that the number of hops in the VPN scenario shows a sharp decrease, then increase above four and finally settling to an average of 3.5 hops. The logic behind this phenomenon is that when the VPN is first established, the packet will be making five hops due to the introduction of VPN_router. However, after the connection is made, the logical network can merely be seen as a direction connection between routerA and VPN_router, effectively bypassing the firewall. Physically it is impossible to make three and a half hops, but this is the time average meaning that hops are fluctuating between three and four. This is because the HTTP application is still making four hops, whereas the database application is making three hops due to the VPN connection.

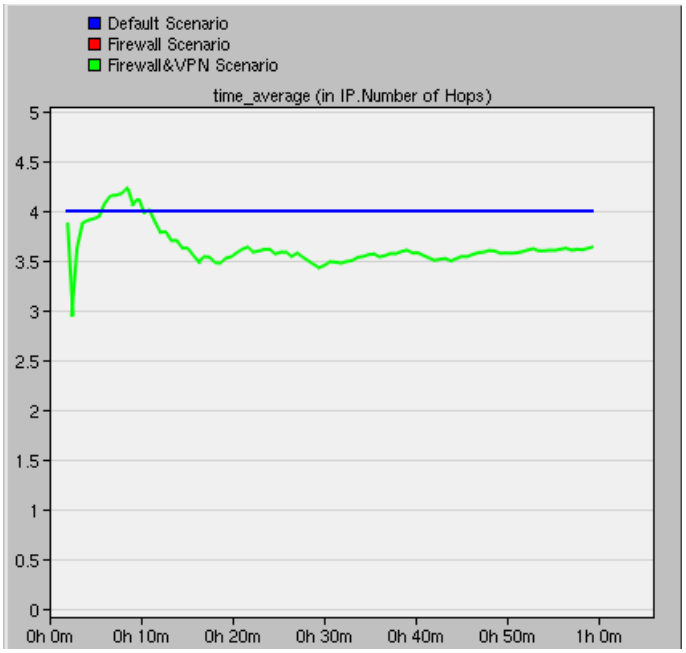

Figure 20: Number of hops

7.0 Future Work

The capabilities of a firewall can only be fully understood when put under high stress. Due to the limited resources of the available hardware, it was not practical to simulate a full-scale real-world traffic model. In the future, it is possible to include a Distributed Denial of Service (DDoS) attack in the simulation. This is to test the ability of the firewall to provide service to authorized users while under extreme traffic load [9]. Several parameters will need to be adjusted to improve the performance of the firewall in a scenario such as different queuing methods like Weighted Fair Queuing (WFQ) and Priority Queuing (PQ). These options are available in the attributes and can be configured by the use of the Quality of Service (QoS) node model in OPNET [1]. The topologies that would be implemented are shown below: the upper diagram shows the inclusion of four attacker subnets, while the bottom shows the internals of each these subnets.

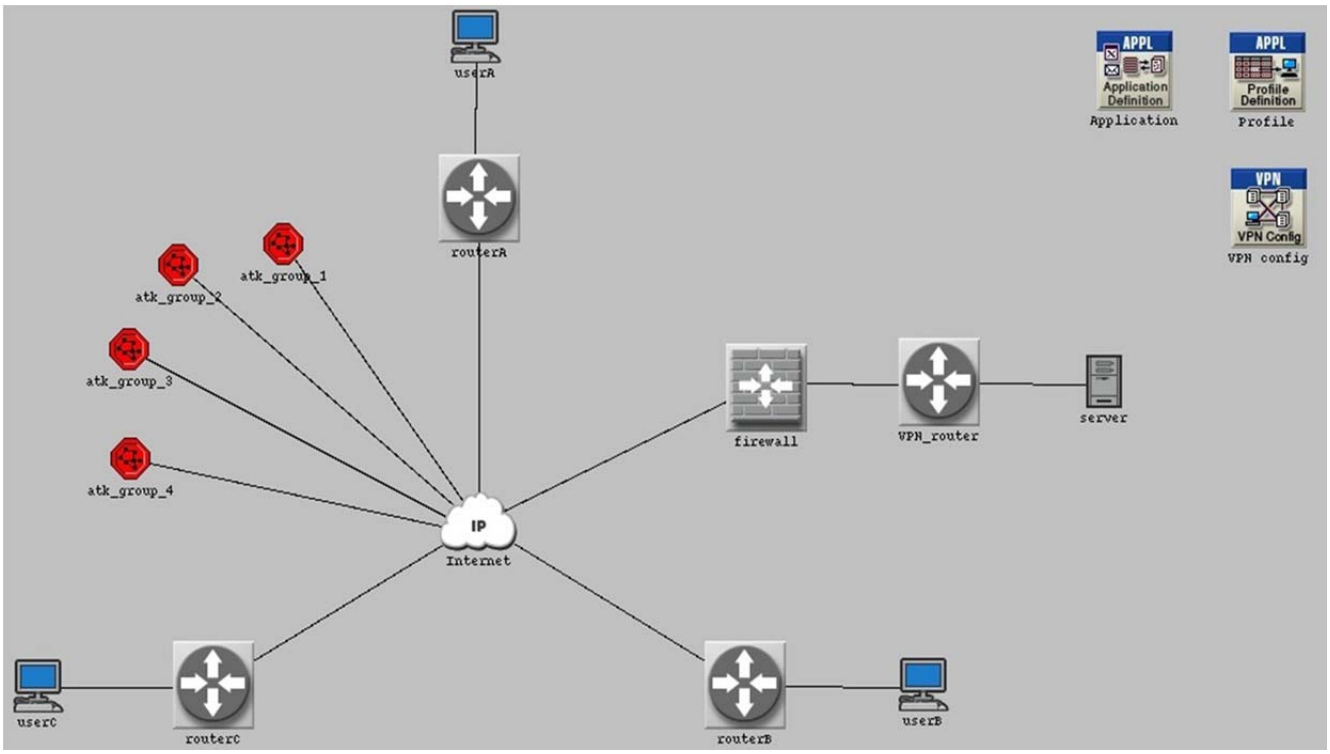

Figure 21: Denial of Service Attack topology

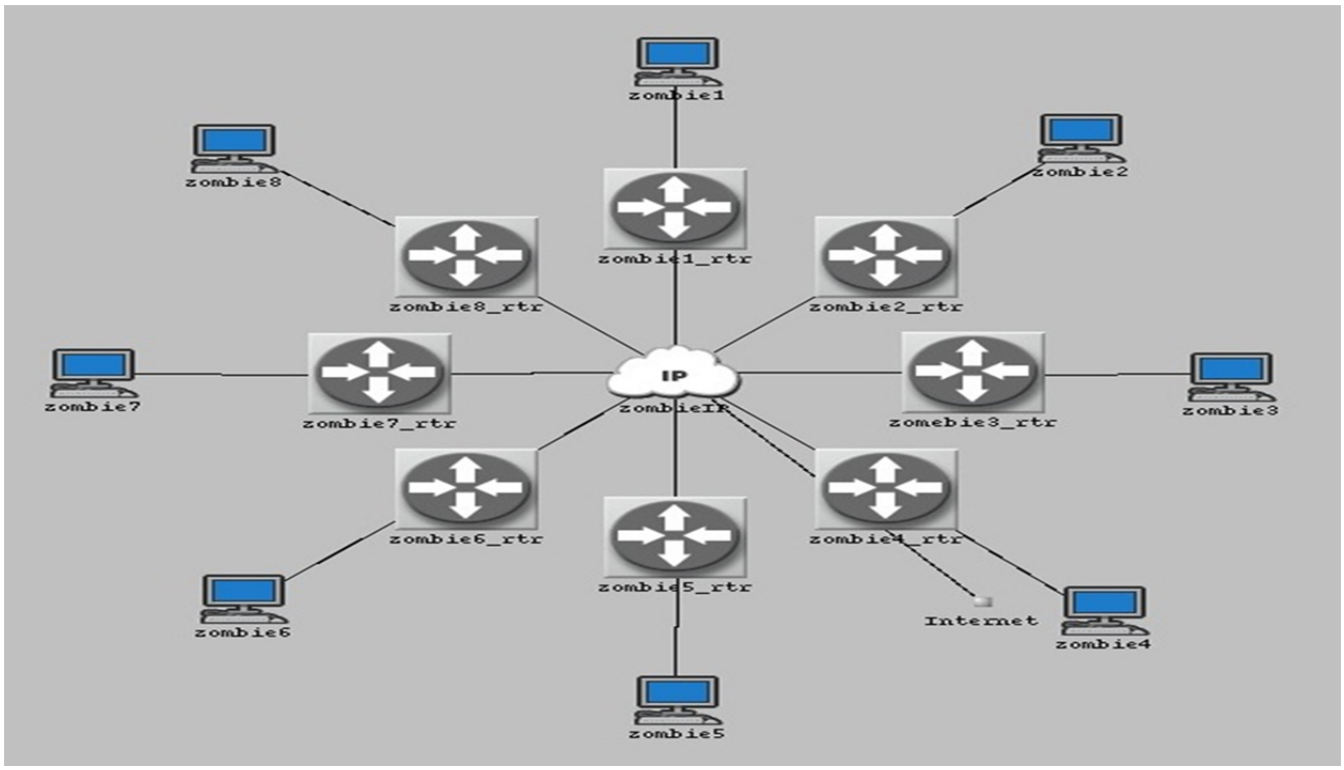

Figure 22: DDoS attacker's subnet

8.0 Conclusion

Firewalls are one of the most standard and effective ways to protect a network from misuse by unauthorized personnel. From the study conducted in OPNET, it can be concluded that they offer reliable security under normal traffic load. There is little end-to-end delay and generally very low jitter, so the use of a firewall will not significantly hinder the performance of the network.

However, many times a user would like to access the services of the protected network and if the firewall blocks a specific application, then no one can use it. To overcome this obstacle, VPNs were introduced. The simulation of the VPN scenario proved that under normal traffic load, it produced very little increments in end-to-end delay and jitter. The percentage increase in application response time, on the other hand, was a fairly substantial 23.33%. The effects of this when scaled to heavier traffic would definitely become a problem, and so limits the types of application that can be efficiently used over a VPN. Video streaming and voice calls would definitely be a challenge, as they require low jitter and end-to-end delay.

In conclusion, firewalls are a very efficient and simple way to protect a network, and are usually the first line of defense. What a firewall cannot do is protect the computer against viruses and other malicious files from infecting the computer, and so it is not the only form of defense a network should have. Anti-virus programs should be used alongside firewalls to provide a wider range of protection. VPNs can provide a secure session in the network without actually physically being in the network, but due to its limitations it is most widely used to perform low bandwidth applications.

References

[1] M. Zhou, "Network Intrusion Detection: Monitoring, Simulation and Visualization" [Online]. Available : http://etd.fcla.edu/CF/CFE0000679/Zhou_Mian_200508_PhD.pdf

[2] Tech-faq. (2012, Feb.) Tunneling [Online]. Available: http://www.tech-faq.com/tunneling.html

[3] Oracle. (2012, March) Configuring Reverse Proxy in Web Server [Online]. Available: http://docs.oracle.com/cd/E19146-01/821-1828/ghquv/index.html

[4] Sapna, M. Sharma, "Performance Evaluation of a wired Network with and without Load Balancer and Firewall", in *2010 Int. Conf. on Electronics and Information Engineering (ICEIE 2010)*, Hoshiarpur, India, 2010.

[5] Y.P. Kosta, U.D Dalal, R.K Jha, "Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network (VPN)" in *2010 Int. Conf. on Recent Trends in Information, Telecommunications and Computing*, Chitkara, India, 2010.

[6] Focus Editors. (2012, March) Types of Firewalls [Online]. Available: http://www.focus.com/fyi/types-of-firewalls/

[7] R. Blair, A. Durai. (2009, May 21). *Chapter 1: Types of Firewalls* [Online]. Available: http://www.networkworld.com/subnets/cisco/060109-ch1-cisco-secure-firewalls.html, p.2

[8]Microsoft. (2012, Feb.) VPNs and Firewalls [Online]. Available: http://technet.microsoft.com/en-us/library/cc958037.aspx

[9] S. Razak, M. Zhou, S.H. Lang, "Network Intrusion Simulation using OPNET," IEEE Computer Design and Applications Repository, University of Central Florida, Orlando, 2002.