12-2016

Router security effect on performance of a network

David L. Leal
The University of Texas Rio Grande Valley

ROUTER SECURITY EFFECT ON PERFORMANCE OF A NETWORK

A Thesis

by

DAVID L. LEAL

Submitted to the Graduate College of
The University of Texas Rio Grande Valley
In partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE ENGINEERING

December 2016

Major Subject: Electrical Engineering

ROUTER SECURITY EFFECT ON PERFORMANCE OF A NETWORK

A Thesis
by
DAVID L. LEAL

COMMITTEE MEMBERS

Dr. Sanjeev Kumar
Chair of Committee

Dr. Jun Peng
Committee Member

Dr. Weidong Kuang
Committee Member

December 2016

ABSTRACT

Leal, David L., Router Security Effect on Performance of a Network. Masters of Science Engineering (MSE), December, 2016, 81 pp., 24 figures, 77 References.

Recently many of the devices that create a computer network offer security to help protect networks from hackers, such as computers, servers, firewalls and even routers. In most cases when protecting a network from hackers having more security is not always the best, because the more resources of the device is used by the security in inspecting connections, and it can compromise performance of the network.

This thesis investigates performance benefit of having security on a router and its impact on the connection rate of the network when it is under security attacks. In this thesis, different security features and configurations offered by the router are tested to see how they affect the connection rate of the network under different security attacks, and compare with the benchmark network performance when there was no security used at all in the router.

DEDICATION

I would like to thank the love and support from my parents which helped encourage me during the completion of my master studies. I would like to dedicate my work to my parents Jose B. Leal and Maria F. Leal, and my brothers, sister, nieces and nephew who inspired me to further my education and accomplish this degree. Without their love and support the completion of my master education would not have been possible.

ACKNOWLEDGMENTS

I would like to formally thank:

Dr. Sanjeev Kumar, Committee Chair and Advisor, for his experienced help in the field of networking and his belief in my abilities. I have learned so much, and this thesis would not have been possible without him. Thank you so much for your encouragement and support.

Dr. Jun Peng and Dr. Weidong Kuang who taught me many thing that were helpful in completing my thesis, and able to make time from their busy schedules to serve as committee members. Thank you so much for your support and guidance.

All of my family and friends, without your support and encouragement I would not have the strength and determination to finish the Master's Program. Thank you all for believing in me and encouraging me to keep going when times seemed so hard.

The Graduate students that I worked with in the NRL LAB, for when we would discuss the technical aspects behind network devices in the lab and their sharing of knowledge that helped me understand more of networks. Thank you so much for your support.

This research work is supported in part by US National Science Foundation under Grant No. 0421585.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER I

INTRODUCTION

In the world of networking, computer hacking has become one of the major growing concerns when it comes to protecting a person's personal information all the way to preventing the internet from being taken down. In many cases people think that hackers are people who use a computer to steal people's information through the internet, but that is not entirely accurate since a hacker is a person who wants to find and exploit the weaknesses in a computer network or computer system [1-6]. Over the years many companies would find ways to improve network security in order to prevent hackers from damaging a computer, server or network. One of the main problems with trying to improve security to prevent Denial of Service (DOS) attacks which consist of Ping attack, and TCP/SYN flood attack is that the increase in security could affect the quality of the network by reducing the speed and connection rate of the computer, server or network that it is trying to protect [7-8]. This is why companies have tried to find ways to add security in different devices that make up a network in different locations, and by doing this they are able to increase network security without having to place too much of a burden on one spot of the network [9-26]. One of the devices used and that we will be looking at is the Juniper J4350 router with Junos Software Release [9.2R1.10] (Export edition) Enhanced Services OS is one of the few routers with its very own built in firewall security [27-28].

This experiment is to understand the configuration of the Juniper Router OS called Junos [29], and it's built in Firewall that can be modified to be used as a Static Packet Filtering firewall or Stateful firewall. We are going to see how the changes in the Juniper router security settings will affect the network in exchange for the protection that it offers for the network.

1.1 Motivation

In the world of networking, computer hacking has become one of the major growing concerns when it comes to protecting a person's personal information all the way to preventing the internet from being taken down. In many cases people think that hackers are people who use a computer to steal people's information through the internet, but that is not entirely accurate since a hacker is a person who wants to find and exploit the weaknesses in a computer network or computer system. Over the years many companies would find ways to improve network security in order to prevent hackers from damaging a computer, server or network. One of the main problems with trying to improve security to prevent Denial of Service (DOS) attacks which consist of Ping attack, TCP/SYN flood attack is that the increase in security could affect the quality of the network by reducing the speed and connection rate of the computer, server or network that it is trying to protect. This is why companies have tried to find ways to add security in different devices that make up a network in different locations, and by doing this they are able to increase network security without having to place too much of a burden on one spot of the network. One of the devices used and that we will be looking at is the Juniper J4350 router which is one of the few routers with its very own built in firewall security. This experiment is to understand the configuration of the Juniper Router OS called Junos [29], and it's built in firewall that can be modified to be used as a Static Packet Filtering firewall or Stateful firewall. We are going to see how the changes in the Juniper router security settings will affect the network in

exchange for the protection that it offers for the network. In the rest of the network we used a simulated server and a single processor Apple iMac Pro Server with an Intel Xenon 2.8 GHz quad-core processor, and had a 12 Giga Bytes of RAM compatible with the operating system Microsoft "Windows Server Enterprise 2012 R2[30]. A Cisco SRW2024 24-port Gigabit Switch which can handle up to 1 Giga bits per second on each port [31].

1.2 Statement of the Problem

Over the years many companies have been creating and selling security features on a lot of their networking products, such as routers to help people think that by merely having these features on the products that their computer networks will be protected from any threat from hackers. In the last decade many companies have noticed that some of the devices that have be sold to improve the security of the network have become a weak link in the network when they become vulnerable when DDoS attacks are sent through the network [1] [32-37].

1.3 Thesis outline

For this thesis I organized the thesis in to five chapters, starting with Chapter I which is an organized introduction, and the motivation for completing the thesis on this topic. In Chapter II we cover the background of how ICMP flood and TCP/SYN Flood DDoS attacks are created and how they affect targeted computers and servers. We also covered the security features of the Juniper J4350 router with Junos Software Release [9.2R1.10] (Export edition) Enhanced Services OS Junos and how the security setting should help protect a network that is under DDoS attacks and why some of these security features are necessary for certain attacks and which ones were not necessary.

When using the Juniper Router which can handle up to 1Giga bits per second of data, we had to create simulated users to help push the router close to the limit of traffic allow able for the router. This help to create a more realistic situation for the network experiment and to have the DDoS attacks to have more of an effect on the router since the attack traffic could only reach a Giga bit per second worth of traffic.

In Chapter III we focused on using a simulated server in the experimental setup of the experiment which had simulated clients on a different network trying to communicate with the server on its very own network. While at the same time we had a separate network sending DDoS attack traffic to the server to see how the router would affect the network when the only form of security on the network is the router. For each attack simulation for the ICMP and TCP/SYN Flood attacks we used a range from 0 Gbps to 1 Gbps with increments of 0.1 Gbps and then recorded the data acquired in Microsoft Windows Excel 2013. For Chapter IV we used the same set of attack traffic as in Chapter III and replaced the simulated server on the network with an Apple iMac Pro Server with an Intel Xenon 2.8 GHz quad-core processor with a 12 GBytes of RAM using the operating system Microsoft "Windows Server Enterprise 2012 R2" server. The Apple iMac Pro Server allowed us to see if the protection offered on the network was from the router or if the firewall on the server was handling most of the DDoS attack traffic. In Chapter V we removed the router from the network and kept the Apple iMac Pro Server in the network while we focused the TCP/SYN flood attack, and when we finished collecting the data from the experiment we compared the results that we acquired from Chapters 3, 4, and 5 that covered the DDoS attacks to see how the router was affecting the network. Chapter VI consists the conclusion for the thesis and our experiments, along with contribution that can be added for future experimentations.

CHAPTER II

DISTRIBUTED DENIAL OF SERVICE ATTACKS

2.1 Background Information on Distributed Denial of Service Attacks

Distributed Denial of Service attack is an improved version of a Denial of Service attack which is used to bring down a network, server, or computer by forcing the victim device to use up its resources to prevent it from working at full capacity [38-44]. When creating a DoS attack a hacker would use his computer to create useless traffic that will ether flood the target with unnecessary traffic or send packet that will confuse the target on what action it should take when deal with that kind of traffic. Now a days most devices such as firewalls and routers contain a DoS attack detection and prevention built in them which search high threshold of traffic coming from a single source [45-46] or if there was a packet or connection that did not seem as if it came from a legitimate source which would mean that server or computer was under attack and then the targeted victim would stop traffic coming from that source. The thing that make Distributed Denial of Service attacks more dangerous is that, while DoS attacks are made from the hackers computer, in DDoS the hacker uses botnets which is when the hacker takes control of unknowingly victims computers and then uses them to created small amounts of attack traffic that will be sent to the targeted victim or server and those small attacks combined will equal one big attack. Since the attack traffic from each source is small the victim will not know that it is being under attack until the victim server or computer is flooded with traffic and has to use all of its resources to stop the traffic and restore itself to full working condition.

Even if the victim computer or server does manage not to be affected by the DDoS attack does not mean the attack was not dangerous, because in some cases the attacks are not meant to bring down the target. When a computer or server is under attack depending on the manufacture and the OS they will deal with certain attacks differently, and this will allow hackers to find out more about the targeted victim and help them to determine which attacks will be most effective against the target. I will cover more on how DoS attacks are used to get more information on a victim computer or server in Section 2.3.4 and how the router helps to protect the router from such attacks.

2.2 Background Information on Different DDoS Attacks

2.2.1 Ping Flood Attack

When dealing with DDoS attacks one of the most common and hard to detect is the ping flood attack. A ping which is also known as an Internet Control Message Protocol (ICMP) echo request [39][40][45] [47-50]which is used by networking specialist as a way to make sure that computer and network devices are connected and communicating with each other. We can see an example of an ICMP packet in Figure 2.1.

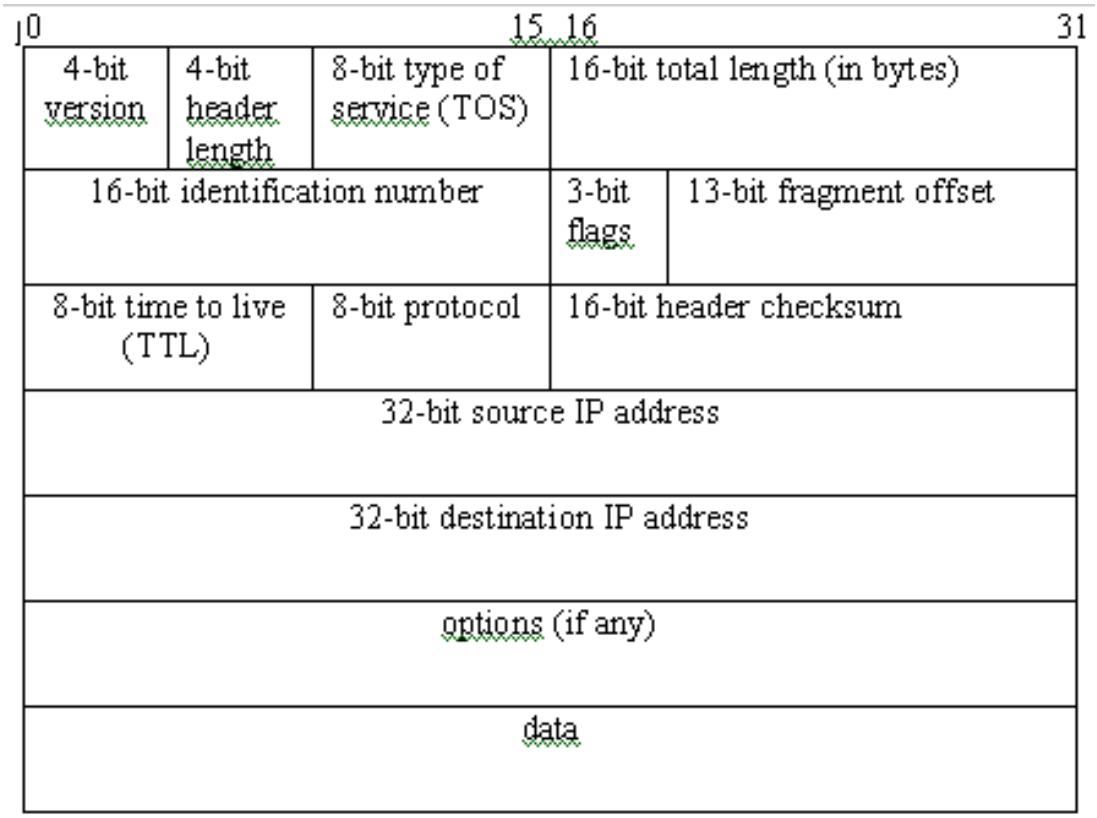

Figure 2.1. IP Header Datagram [51]

Since an ICMP packet is a commonly used method for testing networks most networks do not consider this type of attack to be a threat. The whole point of a ping flood DoS attack is for the attacker to flood the network by sending many ICMP echo request packets to a victim computer or server. Over the years the amount of traffic that a network can handle has increased to Giga bytes which means that attackers would need to send a very large amount of ping traffic to cause any effect to the victim computer/server network. This means the effectiveness of the attack is very dependent on the bandwidth of the attacker's network and the victim's network which means the attacker would need a bigger bandwidth than the victim's network. Otherwise the attacker will have to find other ways to send a large enough attack such as botnets or use other victim computers to help sent the attack.

2.2.2 TCP/SYN Flood Attack

The second attack that we will use will be the TCP/SYN flood attack which the TCP stands for Transmission Control Protocol and the SYN is the name of the flag on the headers of the TCP that are sent to the target, which is where the attacker prevents the completion of the Three Way Handshake as we can see in Figure 2.2 [41] [43] [45] [52] [53] [54] [55].

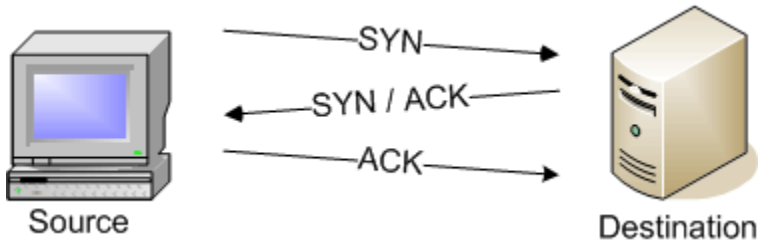

Figure 2.2: Three Way Handshake [56]

The three way handshake is a method for computers to establish a connection before traffic is sent between the computers as shown in Figure 2.2. The three way handshake starts with the client sending a TCP packet to the server; with the SYN flag, which is like the computer asking if the sever can have a connection with the client. The server then replies with a TCP packet that has SYN+ACK flag where the ACK is the server saying that it can make a connection with a client and the SYN is the server making sure if the client can make a connection with the receiver. Then the client responds with a packet that has an ACK flag confirming the connection with the server shown in Figure 2.2. Now the TCP/SYN flood attack is done when the attacker only sends packets with the SYN flag and never finishes the three way handshake by never sending a packet with the ACK flag when the receiver sends a packet with SYN-ACK Flag creating half open connections shown in Figure 2.3.

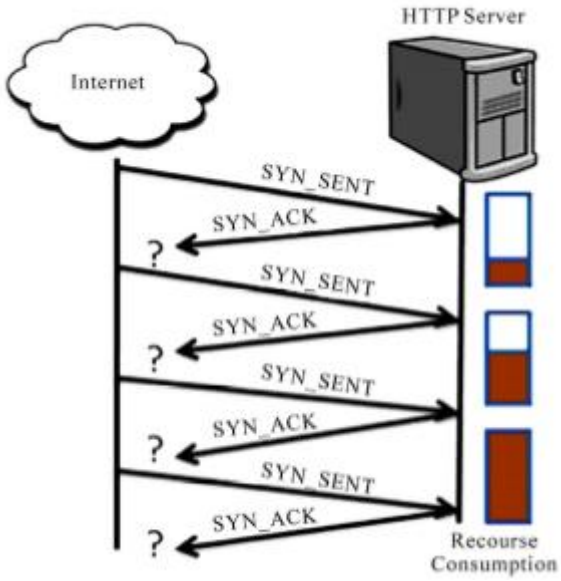

Figure 2.3: TCP/SYN Flood Attack [38]

When the attacker creates these half open connections, this prevents actual users from being able to create connections with the server and consumes the server's resources and reducing the connection rate. One of the extra features offered by the Juniper J4350 Router firewall to help stop TCP/SYN flood attacks other than the threshold for TCP packets is the SYN-Proxy-Proxy which allows the user to set a threshold of how many half open connections there can be in the router. When the number of half open connection reaches the threshold set by the user the router stops the TCP connections between the networks and creates separate TCP connections between its self and the network to make sure that the connections are legitimate connections. If the TCP connections are legitimate the router will establish the connections with the router, but if the three way handshake is not completed between the router and client the connection is dropped before even reaching the network the server is on (Figure 2.4).

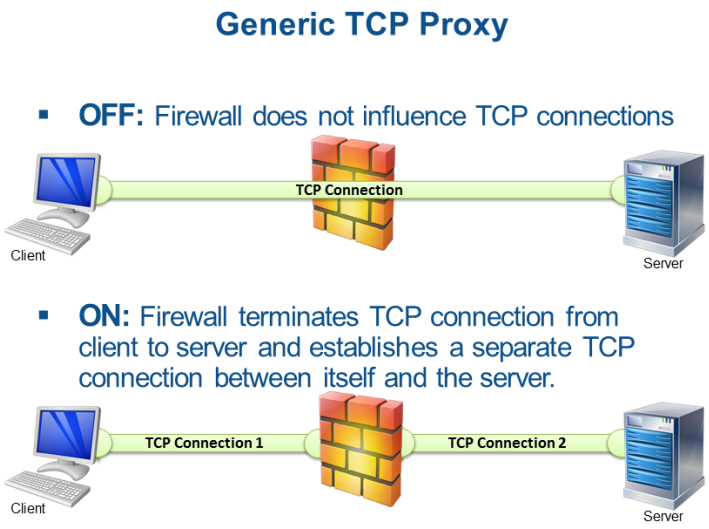

Figure 2.4 Firewall SYN-Proxy-Proxy [57]

2.3 Router Security Offered

When setting up the configuration of many devices manufactures tend to put a recommended setting to help the user to consider what would be a proper setting for new users to use [27][29] [58] - [67] . Most people that set up security configurations that are not too familiar with what protections the security offers and whether they really need the protection end up putting more security than they really need. In most cases having more security may sound good, but is the extra security really worth using more of the routers resources. For this section we will discuss what protection the security offers [45] which we can see in Figure 4 and how the settings should help prevent hackers from harming the network [58].

Section 2.3.1 Scan/Spoof/Sweep Defense

One of the difficulties hacker deal with is finding the location of a victim computer or server that they want to attack, and since they cannot just go up to people and ask for their IP address and Port number they use a method called Sweeping and Scanning. This is a process used to

find locations of computers they can reach from their network, the attacker sends ICMP packets to random IP address or scans for ports. The Juniper J4350 Router uses the scan/spoof/ sweep defense to monitor the traffic that passes through itself and if a single source sends more than 10 ICMP packets to different host or scan for more than 10 ports in the time frame of 5000 microseconds the router will stop letting ICMP packets with that source address from going through the router. This security setting helps make it harder for attackers to find victim computers or servers, and the setting can be adjusted to allow more or less time for 10 ICMP packets to pass through the router with the same source but different destination IP or scan for ports port destination. Although the smaller the time threshold the sooner the attacker can send another 10 ICMP packets or scan for 10 more ports.

Section 2.3.2 MS-Windows Defense

This defense helps protect a computer on a network that uses the Operating System Windows from a DDoS attack known as Win Nuke Attack. An attacker sends a TCP packet to the victim's computer with the Destination Port 139 which is NetBIOS and has the URG flag set which declares the Urgent Pointer field as important. This creates a NetBIOS fragmentation overlap which could force a computer running a Windows OS to crash, and be forced to restart their computer and lose any unsaved data. The Win Nuke attack defense which is part of the MS-Windows Defense will scan for packets with a destination port of 139 and if the URG flag is set then the firewall will unset the URG flag and continue to send the packet. The firewall will mark that a Win Nuke attack was attempted and blocked on the routers log.

Section 2.3.3 Denial of Service Defense

The Denial of Service Defense helps with the protection of the most easily detectable of DDoS attacks, because the attack require making a very noticeable changes to packets that are being sent to create the attack. The changes can be to change the size of the packet to be very large or small, or making and creating many sessions and half open connections. Many networking companies create routers that can easily detect the many of the attack depending on the user, and if the user wants to use the recourses of the router to detect these easy to detect attacks all they have to do is click to turn the settings on. Most of these attacks are the Land Attack, Teardrop Attack, ICMP Fragment, Ping of Death Attack, Large Size ICMP Packet and Block Fragment Traffic. The Source and Destination IP Based Session Limit is to help monitor how many sessions are being created by the source and destination because computers and servers can only handle so many until they begin to close them. Which is why the user can set how many session can be allowed through the router before the router starts closing them to reduce the strain on the victim's network. Next with TCP/SYN attack the hacker creates half open connections by not completing the THREE WAY HANDSHAKE which forces the victim to use up the limited number of connections that are available. The SYN-ACK-ACK Proxy Protection allows the user to set the threshold of how many half open connections can pass through the router, and when the number of half open connections reaches the threshold the router takes the place of the server/computer and waits for the completion of the THREE WAY HANDSHAKE. If the handshake is not completed the router will drop the connection, and if the connection is completed the router will send the connection to the server/computer.

Section 2.3.4 IP Option Anomalies

In some cases hackers use attacks to learn more about their victims Operating System and network, because some OS deal with certain attacks differently than others. When a hacker learns about a victim's network and OS they are able to determine which kind of DDoS attack will be effective in causing the most harm. One of the methods is creating anomalies in ICMP packet header options section which we can see in Figure 2.5, and see what happens. The Juniper routers firewall uses IP Option Anomalies to set the firewall to search the options section of the ICMP header for any unwanted commands such as Bad IP, Record Route, Timestamp, Security, Stream, Loose Source Route, Strict Source Route and Source Route.

Section 2.3.5 TCP/IP Anomalies

TCP/IP Anomalies is used to monitor if there are any strange flag setting in the head of the TCP packet. As we can see in Figure 2.5 there are six flags that can be set on the header of a TCP packet, the flags are used so that the devices on the network know what to do with the connection that is being created such as URG which declares the Urgent pointer field as important, ACK states that the computer received the first packet with SYN flag and more data is being sent, PSH is to push data that is buffered to the receiving application, RST is to reset a connection, SYN which is set on the first packet sent by both computers wanting to create a connection and FIN is use to state the end of data transfer and end the connection. These commands can only be set in certain combinations and if packets are sent with flag setting that could be considered an attack the connection will be closed. The flag combinations that the TCP/IP Anomalies looks for is if the first packet sent does not have a SYN flag, the SYN and FIN flag are both set, a packet with FIN flag set without one with the ACK flag being sent, and a

packet without a flag set. Finally the Unknown Protocol Protection checks to see if the protocol section of the header is 137 or greater otherwise the packet is dropped.

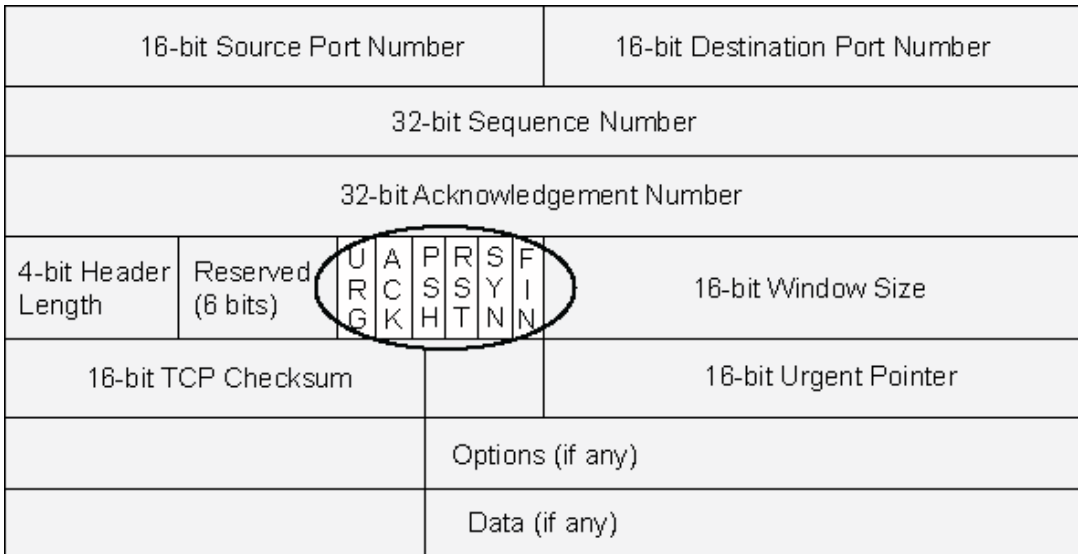

Figure 2.5: TCP Header Flags [68]

Section 2.3.6 Flood Defense

The Flood Defense is as the name suggest where the firewall helps to reduce how many ICMP, UDP and TCP packets will flood the network. In some cases DDoS attacks are not done on purpose, but instead that too many users are trying to communicate with the network due to popularity. This is similar to when a lot of people use a very popular website at the same time and the website runs very slowly. The user uses the settings in the flood defense to determine how many ICMP packets, UDP packets and TCP packets with the SYN flag can pass through the router per second. Since the TCP packets are used to create connection the Flood Defense also monitors the number of connections.

2.4 Chapter Summary

In this chapter we explained what a Denial of Service (DoS) attack is and the improved version of DoS attack which is known as Distributed Denial of Service (DDoS). The DDoS attacks are more dangerous do to that fact that the attack is created by using a combination of different sources to cause harm to the same target source which makes them harder to detect than DoS attacks. We also explained the ICMP Request packet flood attack and the TCP/SYN flood attack and how those attacks cause trouble for the network and that we will be using for the experimentation in this thesis. The Security features of the Juniper J4350 router were reviewed to explain how we used the different security features to create the different security settings that will be used during the different experimentations for the this thesis.

CHAPTER III

COMPARISON OF NETWORK PERFORMANCE USING ROUTER WITH DIFFERENT SECURITY SETTINGS

3.1 Introduction

The purpose of this lab was to understand and see how the Juniper J4350 router with Junos Software Release [9.2R1.10] (Export edition) Enhanced Services OS Junos with built in firewall would help a network that is under Distributed Denial of Service (DDoS) attack [69] [70]. We first started by using [29] [58] [59] [60] [61] [62] [71] to help us configure the router to be able to interact with the networks that we wanted to work with as shown in Figure 3.1. Since the router was able to have the firewall act as a Stateless or a Stateful firewall, we chose to configure the router as a Stateful since that is one of the most common firewall configuration used today. This allowed the router to use flow base forwarding and worked more in handling with the connections that are going through the router instead of monitoring every packet, and allowed us to use the security features that we discussed in Chapter II and to create the trusted and untrusted zones for the networks that are connected to the router, this also allowed us to set different levels of security for the different networks depending on how trust worthy they were. We created three subnetworks where one of them will contain simulated users on 192.168.2.0/24 with the range of 192.168.2.1-192.168.2.254 that want to communicate with a web server that will be located on the subnetwork 192.168.3.0/24 with the IP address of 192.168.3.2.

Then we used the remaining network 192.168.1.0/24 as the network being used by the hackers that are trying to send attack traffic to the server and allowed us to have the attack traffic use random IP and MAC addressing that would fall in the 192.168.1.0/24 network range. The experiments would start off with having the clients communicate with the simulated server for 7 minutes without DDoS attack traffic being sent in the network. Then we would start sending the attack traffic through the router and to the simulated server, while we would increase the DDoS attack by 1% of 1 Gbps after letting each attack size run for 5 minutes until the attack rate reached 1 Gbps. Then we allowed the test to run for 3 extra minutes to allow any remaining connection to finish traveling through the network, which had each test running for 110 minutes or 1hour and 40 minutes. This setup would mean that the networks have to go through the router in order to communicate with each other as we can see in Figure 3.1. The simulated clients and the server networks were placed on the trusted zones and were not given that much security when they send traffic through the router, which is similar to employees of a company communicating with the server owned by the company in the companies very own building. While the networks that are sending the attack traffic is placed in the untrusted zone and given more security setting when they try to communicate with network on the trusted zone. As mentions in the previous chapters ICMP packets are a common tool used to test network to make sure that they are working to the best efficiency, but even then many firewalls are able to prevent ICMP packets from passing through the devices that use the firewall by making adjustments to the policies placed on the router. The questions still remains if the solutions to prevent Ping Flood attack is really the best solution to prevent the attack from reaching the attack target, because setting this type of solution still requires the consumption of the routers resources to identify the ICMP packet that are passing through the router. In order to initiate this type of

security feature the router had to be configured to use flow based forwarding which is commonly used in routers now a days instead of packet based forwarding [72] [73].

When dealing with the security setting of the router we will be referring to four different setting known as No Security, No PING through, Default, and Default Everything. The security setting called NO Security is as the name suggests, and where we no security is activated to check the traffic that is passing through and allowing all connections to pass through the router including attack traffic. The next security setting would be the NO PING Through in which the policies of the router are configured to prevent and ICMP packets from passing through the router, but would still have the router check all the traffic that pass through to determine which traffic is ICMP packets. When using the Default security setting the router will only be allowed to use firewall protection that relates to the type of attack that is being used in that experiment with the setting recommended by the Juniper company, so if TCP/SYN flood attack is being used the router will only be able to protect against TCP/SYN attack traffic and no other attack. In the final security setting Default Everything the firewall will be configure to protect the network against all types of attack even if the attack possess no harm to the network such as the WIN nuke attack which does not harm the devices but only helps attackers determine the type of software used by the target. The values used in setting the Default Everything were the settings recommended by the Juniper Company when using this router model.

Configuring the router to work in flow based forwarding was the only way to configure the policies to have the router prevent ICMP packets from passing through the router, but even if the ping packets are prevented from entering the network the larger the DDoS ping flood attack the more rescores are consumed, by the router to scan for ICMP packets and block them form

passing through, that makes it slower for the authentic traffic to pass through the router and can cause the connection to time out and results in the loss of the connection this security method is "NO PING THROUGH".

The next security settings would be to set the recommended level of security that is requested by the router to prevent any and all forms of DoS attacks and different versions of those attack that would travel through the router. This means that the router will also be configured to protect against TCP/SYN flood attacks and other kinds of DDoS attacks while the experiments will only be testing to see how the router handles ICMP flood attacks, and this security method will be considered as "Default Everything". Since this security setting is also configured to protect the network from TCP/SYN flood attack, this security setting will also be used for the section of this chapter when using the TCP/SYN flood attack to see how this setting will handle any situation.

The third security setting is similar to the setting Default Everything except that this setting was configured to focus on protecting the network for the attacks that we were testing in the experiment. The main purpose of this setting is that in some cases the DDoS attacks that are used do not harm the network, but are used to test and see what kind of Operating System is being used in the network by how the OS deals with that type of attack. This should help the router reserve more of CPU and memory to be used against all of the more dangerous DoS attacks, and this security setting is called "Default". For the final test of the experiment was to have no security settings set on the router while the network was under DoS attacks, because this allowed us to see how the attacks were affecting the network to get a better understanding of how the security setting are helping the network.

For the experiments using the TCP/SYN flood attack we had to make changes to some of the previously mentioned security setting that were being used for the ICMP flood attack, since the Default Everything security setting already had protection for all types of DoS attack including ICMP and TCP/SYN attacks the setting remained the same for both DoS attacks. When having no security on the router does not differentiate between the different types of attack the configuration for the security setting No Security will also be used for the TCP/SYN flood attack. Unlike the ICMP flood attack we cannot configure the router to prevent TCP traffic through the router even though the policies on the router will allow us to make that kind of configuration. In chapter II which explains that the TCP/SYN flood attack works by creating half open connection which lowers the number of connections available for the clients, but when dealing with web servers the clients send TCP packet to the server to create connections between the two and allows data to be sent faster. This mean that if we configured the router to prevent TCP traffic form going through the router, then that would also stop all traffic from passing through the router making the situation similar to as if we removed the cable that connects the router to the simulated web server. That is why that security setting was not used in the TCP/SYN flood attack experiments as you can see in section 3.4.2. The final change made in the security settings for the TCP/SYN flood attack experimentation was to the "Default" security settings, because as mentioned earlier the Default setting was configured to focus on protecting the network from the DDoS TCP/SYN flood attack that is being tested. The changes that were made to the Default setting were to have focus on mitigating the TCP/SYN flood attack instead of the ICMP flood attack. During the test of the TCP/SYN flood attack we will focus on the three security setting Default Everything, Default (for TCP/SYN), and No Security.

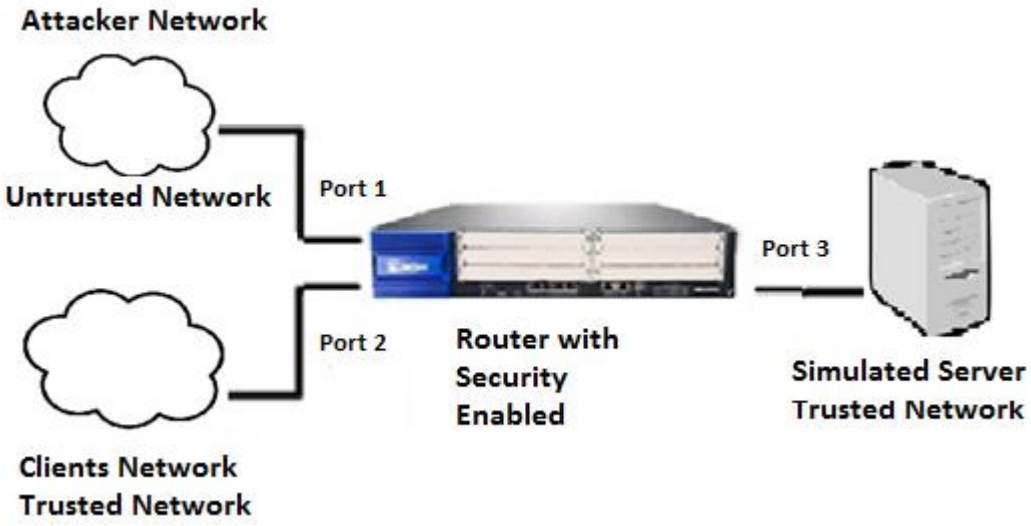

Figure 3.1: Experimental Setup for Juniper Router with Simulated Server

3.2 Experimental Setup

3.2.1 Hardware

Router:

The Juniper J4350 router [28] [69] that was used is one of the J series with 4 fixed Giga Ethernet ports which support gigabit networking, has a built in firewall, uses the OS Junos, and has a built in:

Processor- to run the JUNOS internet software and maintains the routing protocol and routing tables. The processor also create the packet forwarding switch fabric used by the router.

DRAM- provides storage for forwarding tables, routing tables, other routing engine processes, and is used to buffer incoming packets

EPROM- where the serial number of the routing engine is stored.

Crypto Accelerator Module- the cryptographic algorithms that are used by the IPsec (IP security) services, are enhanced by the processor card. The supported algorithms are AES, 3DES, DES, HMAC-MD5, and SHA-1.

Compact flash- the primary storage for microcode, configuration files and software images, which is kept in a slot on the motherboard of the router.

3.2.2 Software

The software used by the Juniper Router is the Junos Software Release [9.2R1.10] (Export edition) Enhanced Services OS, and Microsoft Excel 2013 [74] was used to record the collected date form the performance monitor of the router and the simulated web server and create the graphs for the data.

3.3 Parameters of Performance Comparison

In this chapter of the thesis we will be comparing the connection rate of successful connections received by the simulated web server and the CPU Utilization of the Juniper J4350 router.

Connection Rate (connections per second) – This allowed use to keep track of how many connection were created between the simulated server and the simulated clients through the Juniper Router, and monitor how many of the 10,000 connections per second being sent between the two are being dropped because of the DDoS attack.

CPU Utilization- the central processing unit was the second most important parameter to record during the experiments of this chapter. This allowed use to see how the attack traffic was affecting the router and see how the router was able to handle the stress.

CPU User Usage (%)- The router only used the User Usage when the Idle Time showed that almost all of the CPU remaining resources was about to be used in an attempt to control the traffic that was going through the network and preventing the attack traffic from passing through to the router.

CPU Real Time (%)- The Real Time of the CPU allowed us to record how much of the CPU's resources were being used when the DDoS attacks were being sent, and at what size of the attacks were forcing the CPU to consume most of the resources. This also allowed us to see how much of the routers resources were still unused during the DDoS attack throughout the network to show how close the router was to use the User Usage %.

3.4 Results and Discussions

For this section we gathered the data of the connection rate that we obtained in the tests and compared them to see which security method offered the best connection rate to the network for the simulated users. One of the problems that we encountered during the test was that sometime when the attacks would reach high enough the baseline connection rate was affected as seen in Figure 3.2 which is the baseline before the attack.

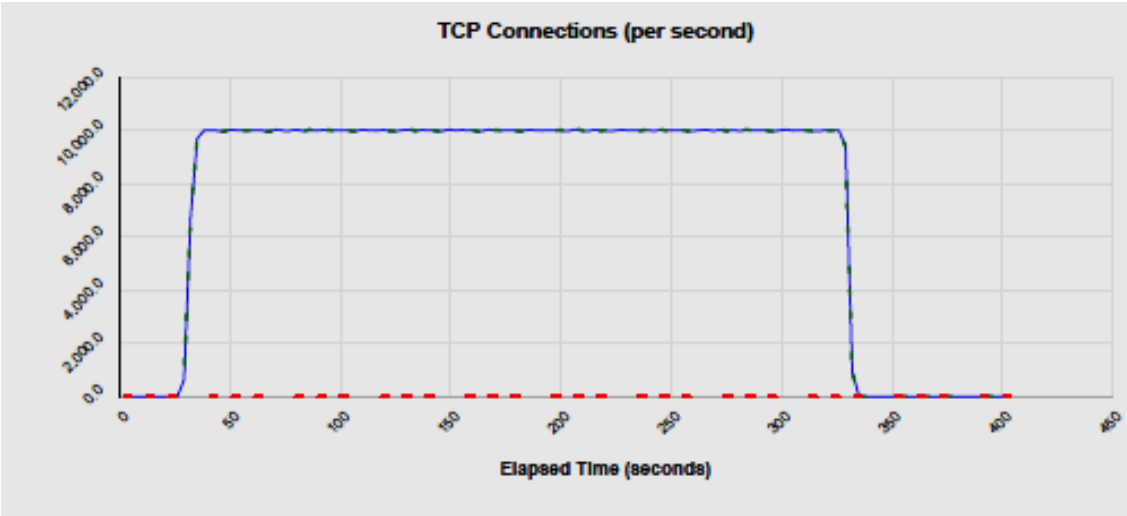

Figure 3.2: Baseline without any DDoS attack

In normal cases the network should have shown errors through either the users or the server, but both showed that there was no error. This was showing that with the used of random MAC addresses along with random IP addresses would cause the ARP table to fill up, and would make things difficult for the router to store new addresses. We had to clear the ARP table after every complete experiment to make sure that the ARP table would not affect the experiment results.

3.4.1 Ping Flood Attack

In order to get a better understanding on how preventing ping traffic from entering the router would affect the connection rate of the legitimate users, we also ran a test that would allow ping traffic through the router without having the security activated to represent the baseline for the network which turned out to be 10,000 connections per second. Then we recorded the connection rate of the network as the attack traffic was sent through the router, and recorded the connection rate in Figure 3.3. As we look at the connection rate of each network using the different security settings, we can see that there was not much of a difference between the four security setting as the results kept fluctuating between which one was the best. This also meant that using the

security setting NO Security was able to give the same results as if all of the firewalls security was activated. This does not leave out the fact that even if it was giving close to the same connection rate, using NO Security could be forcing the router to use up more resources to have that kind of connection rate.

Next as we take a look at Figure 3.4 which show the Real Time Usage of the Juniper Routers CPU we can see that by the attack speed of 20% of 1 Gbps the router was close to using up almost all of its own resources with all of the attacks which shows that most of the loss of the connection rate that was happening in Figure 3.3 from the attack speed of 20,000 Mbps and up in the network was happening at the router. In Figure 3.4 we can see that all four security setting used for the ICMP flood attack were all consuming close to the same amount of resources throughout the tests and could lead some people to think that if all the security setting are affecting the router in the same way then it does not matter how much security is place on the router as long as everything is protected.

It is not until we look at Figure 3.6 that we can see the big difference between the four security settings and how they are having an effect on the router. As mentioned Section 3.2 the CPU User Usage show when the router is unable to handle the use of its resources and tries to reduce the stress that is placed on the router and then when we look at the next increment of DDoS attack speed in Figure 3.4 we can see that the Real Time Usage would decrease by a little which explained how the four security settings would seem to be consuming close to the same amount of resources. We are able to see in Figure 3.5 that the security setting of "Default" and "NO Ping Through" forced the router to be pushed to the limit at a low DDoS attack speed of 10,000 Mbps and 20,000 Mbps. While the Default and No Ping Through put the most strain on

the router, the security setting for Default Everything and No Security only put a strain on the router when the when the DDoS attack traffic reach 60,000 Mbps and 70,000 Mbps with the No Security setting performing the best of the four security settings.

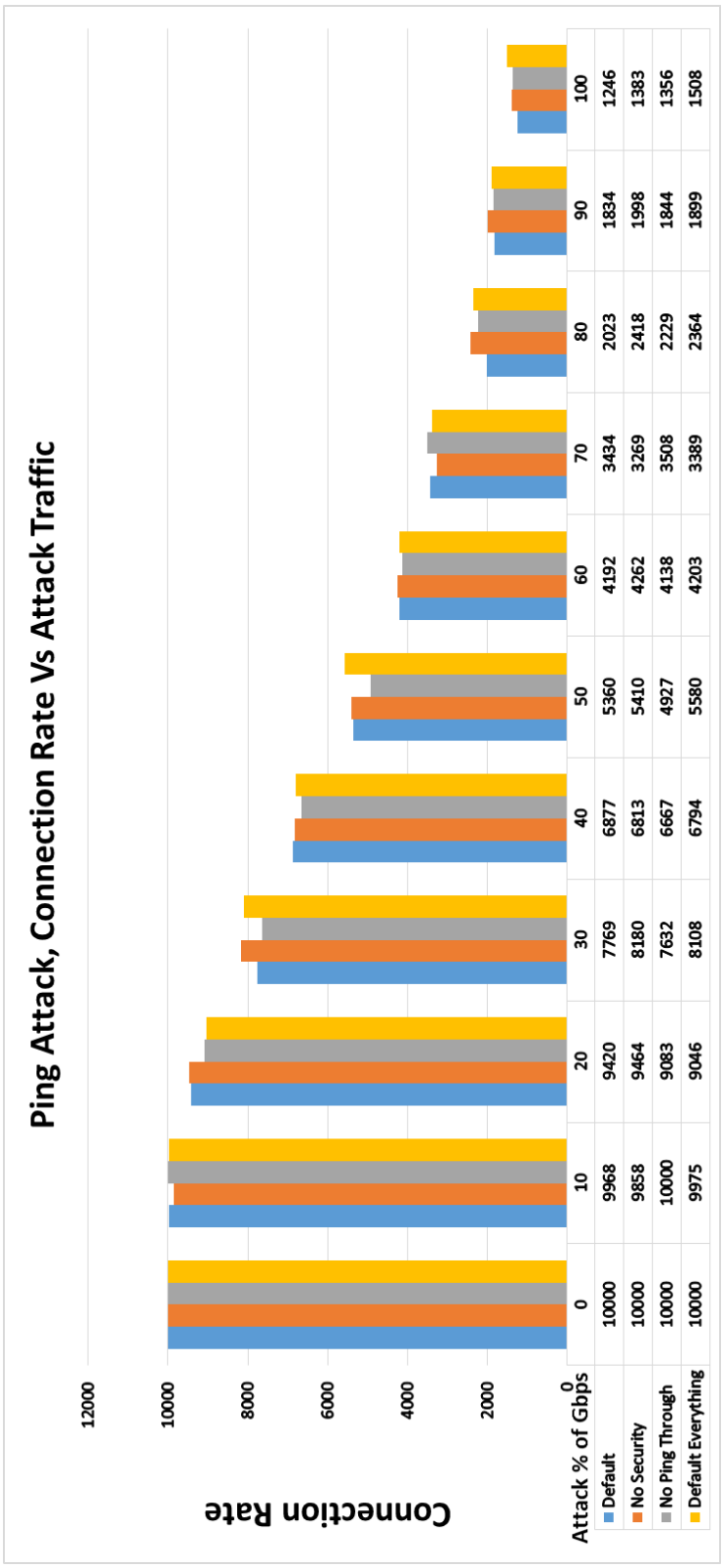

Figure 3.3: Comparison of Security Setting for ICMP Flood Attack Connection Rate

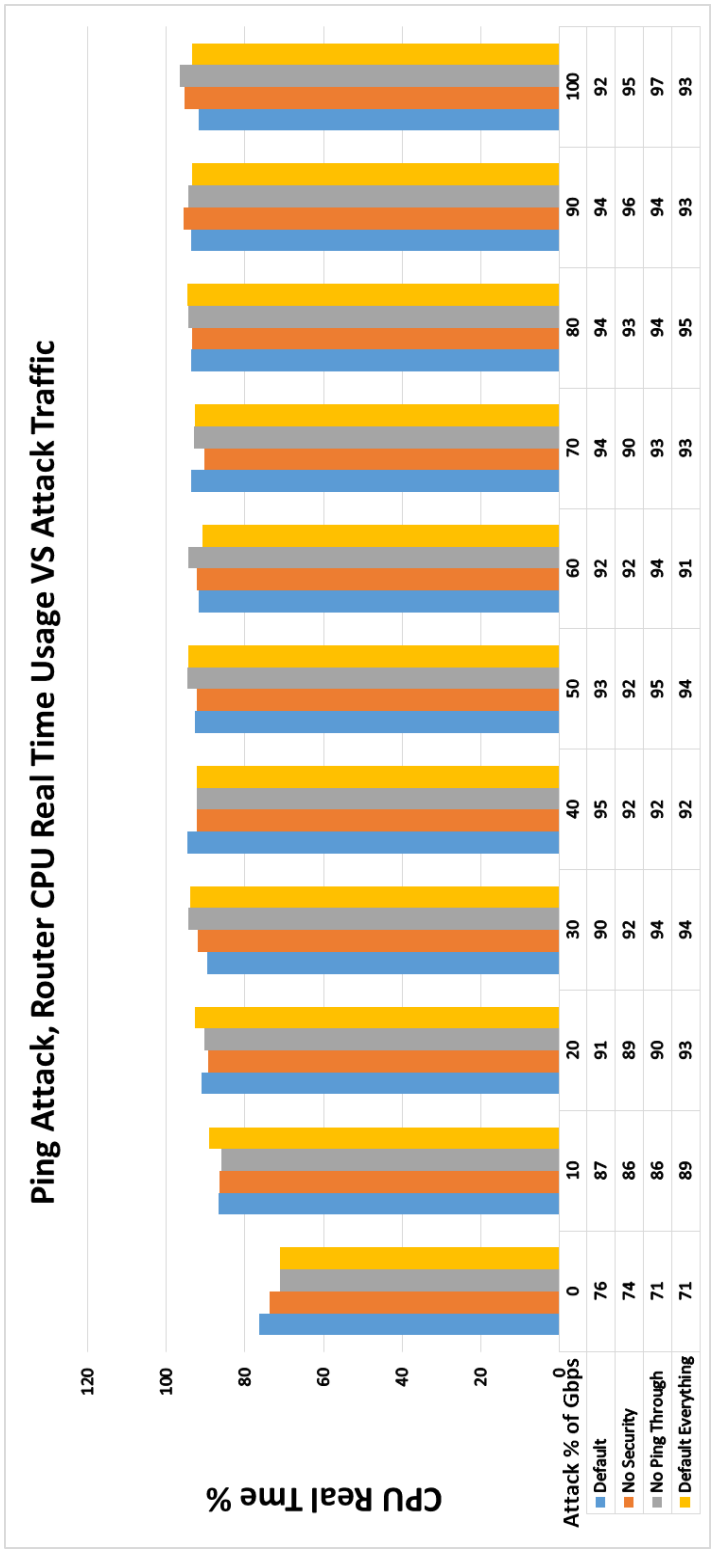

Figure 3.4: Comparison of Security Setting for ICMP Flood Attack CPU Real Time Usage

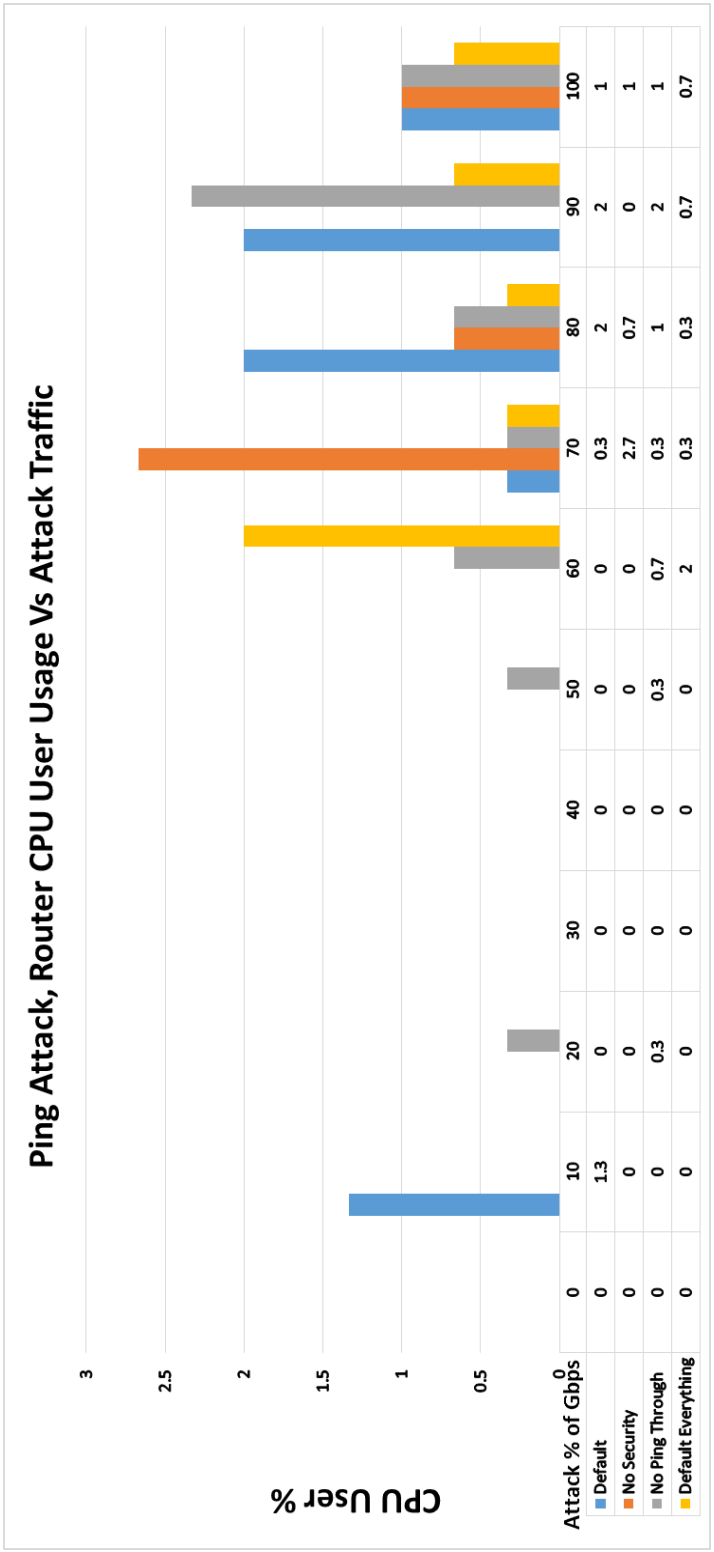

Figure 3.5: Comparison of Security Setting for ICMP Flood Attack CPU User Usage

3.4.2 TCP/SYN Flood Attack

The first thing we had to consider was the removal of the security setting that would prevent any form of traffic that resembled a similarity to the attack traffic from entering, because when dealing with a web server almost all communication between a web server and any other devices begins with creating a connection. A completion of the three way hand shake is necessary for creating connections, and the TCP/SYN Flood attack creates the first half of the three way hand shake and prevents the completion of the rest. If we configure the Juniper router from allowing TCP traffic from entering the router, we would just end up stopping any connection from entering the network which the server is on, and this would be the same as removing the Ethernet cable that connects the router to the server.

As we look at Figure 3.6 we can see that the TCP/SYN flood attack created a greater loss of the connection rate than the Ping flood attack showing how more dangerous the TCP/SYN attack is in comparison.

Unable to use the security setting of preventing and TCP traffic from passing through the network, we were left with only three remaining security setting for the TCP/SYN flood attack. The experiments were simulated and recorded in Figure 3.6 where we have blue for Default Security, Red for NO Security and yellow for Default with Everything Security. The connection rate of the three security methods reach half at 30,000 Mbps showing that the TCP/SYN flood attack has more of an effect on the network than the ICMP flood attack which did not get the network connection rate to drop by half until the attack reached 50% to 60% of the 1 Giga bit per second. Throughout the experiment using the TCP/SYN flood attack the connection rate between the three security setting the results show that there was a small difference between the connections created. Since the three different security settings did not have much of a difference

on the security people could use the Default Everything security setting which would help against the other DDoS attacks that are used to gather data about the networks. The question still remains on how much of a strain is placed on the router due to the use of these security settings, and which one is really helping the router to protect the network while under the DDoS attack. Next as we take a look at Figure 3.7 which show the Real Time Usage of the Juniper Routers CPU we can see that by the attack speed of 20% of 1 Giga bps and similar to the ICMP experiment in section 3.4.1 the router was close to using up almost all of the resources available to the router with all of the attacks which shows that most of the loss of the connection rate that was happening in Figure 3.6 from the attack speed of 20,000 Mbps and up in the network was happening at the router which could mean that the router is preventing the attacks from reaching the server and preventing the server from suffering any problems. In Figure 3.7 we can see that all four security setting used for the TCP/SYN flood attack were all consuming close to the same amount of resources throughout the tests and again could lead some people to think that if all the security setting are affecting the router in the same way then it does not matter how much security is place on the router as long as everything is protected.

When we look at Figure 3.8 we can see the big difference between the three security settings and how they are having an effect on the router. As mentioned Section 3.3 the CPU User Usage show when the router is unable to handle the use of its resources and tries to reduce the stress that is placed on the router by either dropping the connection or some of the attack traffic passes through the router. Then when we look at the next increment of DDoS attack speed in Figure 3.7 we can see that the Real Time Usage would also decrease as in section 3.4.2. In Figure 3.6 we are able to see that the security setting of “No Security” and “Default Everything” forced the router to be pushed to the limit at a low DDoS attack speed of 10,000 Mbps and 30,000 Mbps.

While the No Security and Default Everything put the most strain on the router, the security setting for Default only put a strain on the router when the when the DDoS attack traffic reach 50,000 Mbps with the Default security setting performing the best of the four security settings.

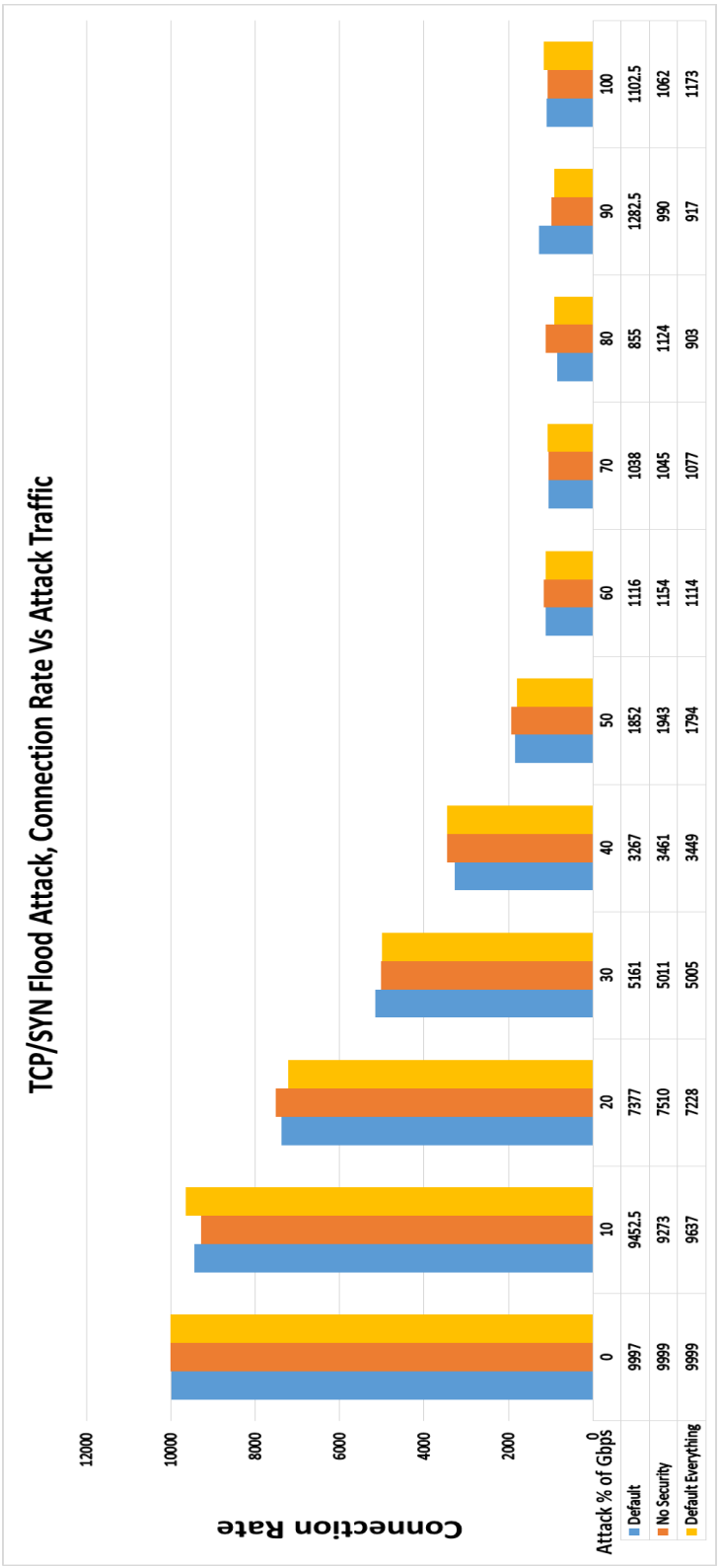

Figure 3.6: Comparison of Security Setting for TCP/SYN Flood Attack Connection Rate

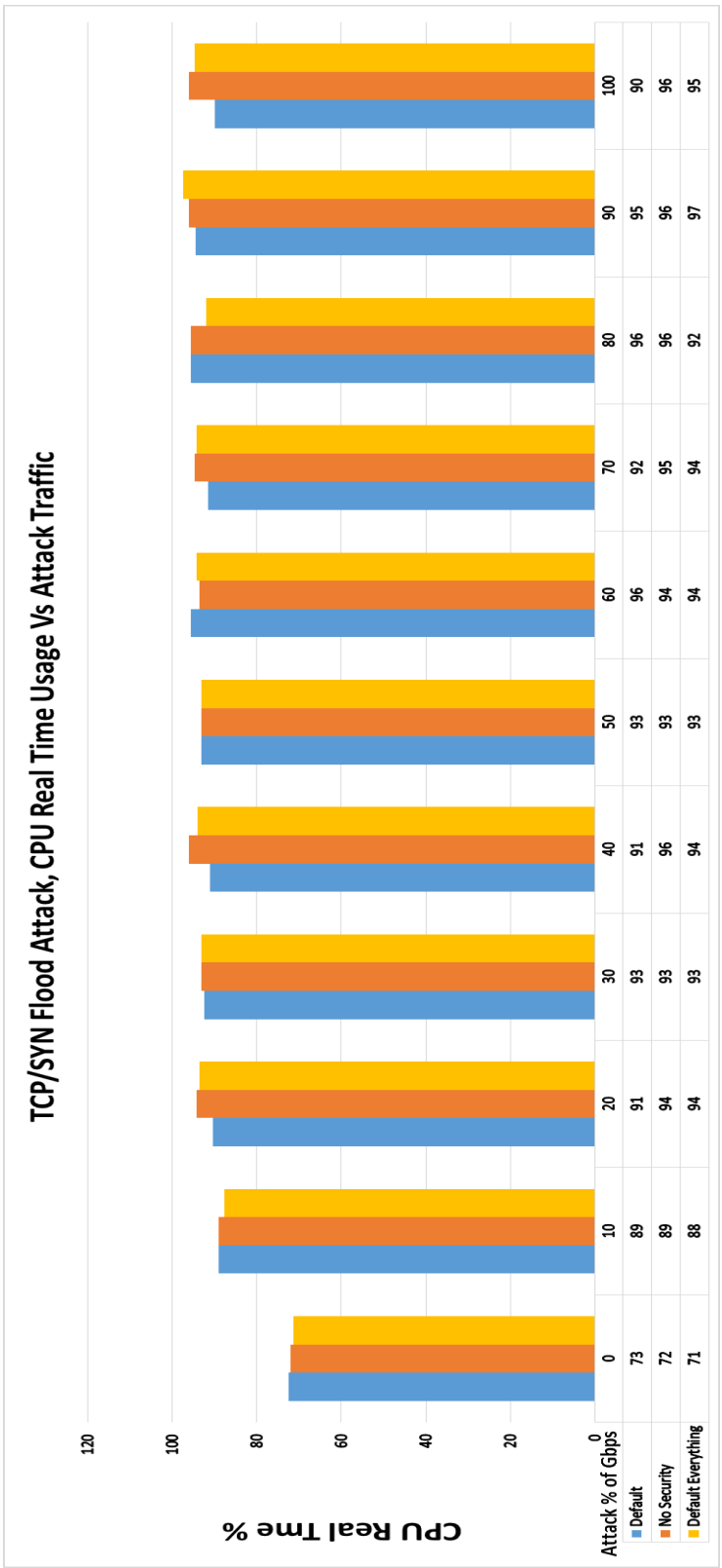

Figure 3.7: Comparison of Security Setting for TCP/SYN Flood Attack CPU Real Time Usage

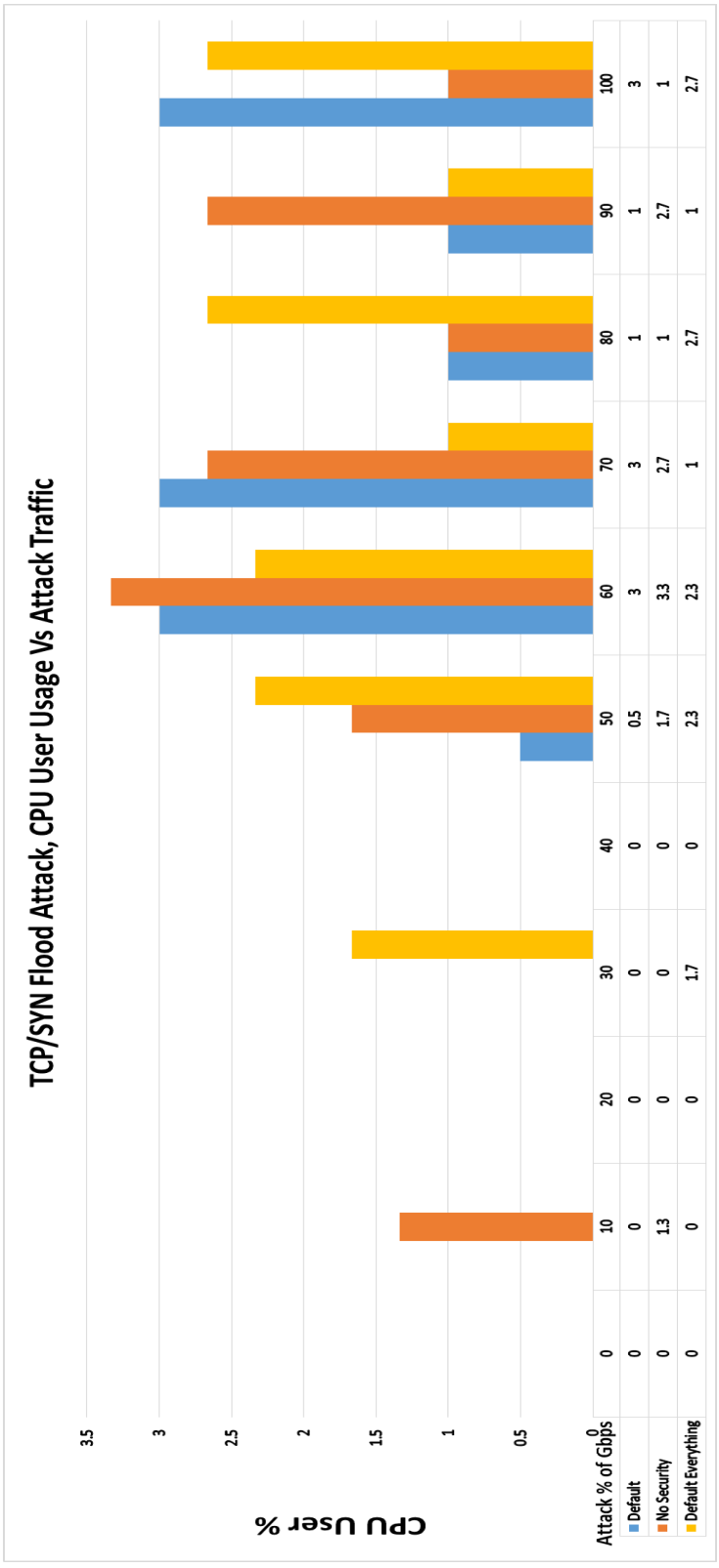

Figure 3.8: Comparison of Security Setting for TCP/SYN Flood Attack CPU User Usage

3.5 Chapter Summary

As we review the results that we gained from the ICMP Flood and the TCP/SYN Flood attack experiments that were simulated in this chapter to test the limitations of the router by using a simulated clients and server. After all the testing and collection of the data form the router and the server, we were able to see that when we look at the connection rate most of the attack did not show much of a difference in the drop of the connection rate from the different security setting that were used on the router. When we took a closer look at how much of a strain that the DDoS attacks were putting on the router by observing the CPU User Usage we were able to see that there was a much greater difference on how the different security setting were having on the router. For the ICMP flood attack the results showed that using the Default security setting forced the router to be pushed to its limits at only 100Mbps, as was followed by the security setting that prevented the ICMP packets from passing through the router which caused the router to use the CPU User Usage when the attack reached 200Mbps. This showed that these two would be the least affective in helping to protect the network during a DDoS ICMP flood attack, while the Default Everything and the No Security did a little better even though the loss in the connection rate was nearly similar to the other two during the lower half of the attack range. In the TCP/SYN flood attack we noticed that in Figure 3.6 the three security settings did not have much of a difference when it came to protecting the connection rate in the network which could be misleading for those who are not too familiar with configuring security settings. In Figure 3.8 we were able to get a better understanding between the differences of the three security setting which showed that the NO Security setting ended up putting more of a strain on the router by forcing the router to drop connection at an attack of 10% of the 1Gbps. This was followed by the Default Everything security setting pushing the router to its limits at an

attack of 30% of the 1Gbps, which meant that the security setting Default was able to help protect the network with the same efficiency as the other two and put the less strain on the router.

CHAPTER IV

COMPARISON OF NETWORK PERFORMANCE USING A SERVER WITH MICROSOFT'S WINDOWS 2012 ENTERPRISE R2 WITH AND WITHOUT FIREWALL

4.1 Introduction

For the experiment, we configured the Juniper J4350 router with Junos Software Release [9.2R1.10] (Export edition) Enhanced Services OS Junos in a star topology network as seen in Figure 4.1, and used Category 6 Ethernet cables to connect all the network devices.

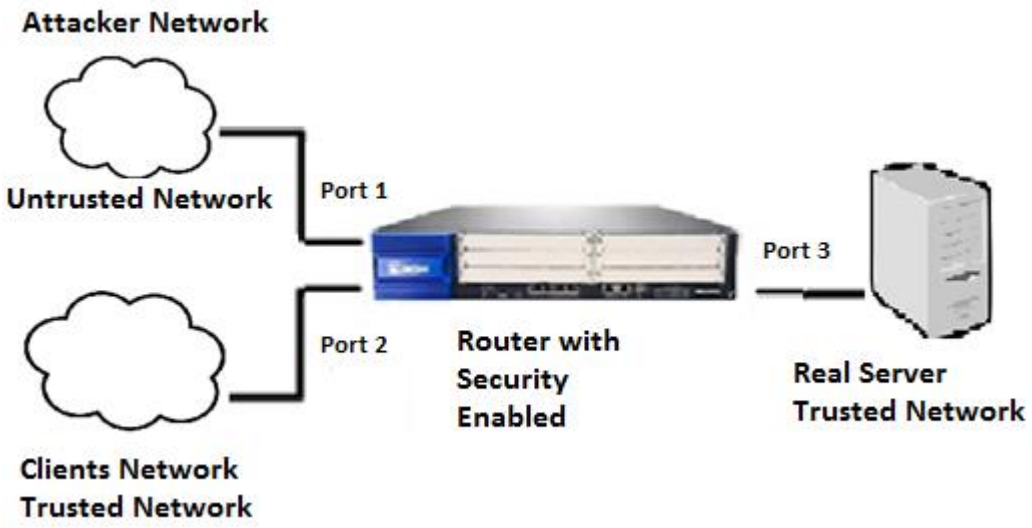

Figure 4.1: Experimental Setup for Real Server with router.

We first started by using [29] [58] - [62] to help us configure the router to be able to interact with the networks that we wanted to work with as shown in Figure 4.1. We configure the router as a Stateful since that is one of the most common firewall configuration used today that allowed the router to use flow base forwarding and worked more in handling with the connections that are going through the router instead of monitoring every packet as in Stateless configuration. Since the Juniper J4350 router is able to handle up to a Gigabyte per Second of traffic at each port which is why we used two networks to simulate TCP/SYN attack on the 192.168.1.0/24 network and then had the network labeled as untrusted, while we kept 192.168.2.0/24 and 192.168.3.0/24 networks containing the server and simulated clients on the trusted zone. Network 1192.168.2.0/24 was used by the simulated clients and the server was placed on network 192.168.3.0/24. The attacking network was placed on a different network to allow us to simulate DDoS traffic that would use random source MAC and IP addresses with in the network range without causing collisions between the legitimate traffic and the attack traffic, and used a more real world DDoS attack traffic which will make it even harder for the router to stop the attack traffic. In Chapter 2 we were able to see that using the Security Setting "Default Everything" did not always give the best results on the works connection rate it was still very close, and in most cases many users would sacrifice a little bit of the quality for quantity we decided to use it on the router for this chapter. Using the Default Everything security setting as the only security setting on the router would mean than any changes on the network performance would be cause by any changes made to the server. Next we configured the Apple iMac Pro Server with an Intel Xenon 2.8 GHz quad-core processor with a 12 GBytes of RAM using the operating system Microsoft "Windows Server Enterprise 2012 R2" server on network 192.168.3.0/24 to work as a web server that allowed us to use http traffic, and the legitimate

users on client network 192.168.2.0/24 would use the GET command to retrieve a 1 byte web page from the server. Using the smallest size web page allowed the router to handle a higher connection rate baseline, which was 10,000 Connections per Second when there was no attack traffic. The attack network was used to create ICMP Echo Request and TCP/SYN flood attack that ranged from 0 to 1 Gbps with increments of 0.1 Gbps with random source MAC and IP addresses and was sent to the server on network 192.168.3.0/24. For the first test in the experiment we started with using the Apple iMac Server and compared the performance of the server with and without the firewall activated and compared the connection rate of the network along with the routers CPU performance while the network was under an ICMP echo request flood attack. The we chose to leave the server with the option of the firewall that gave the best results and compared the real server against the simulated server on a network that under a stronger DDoS attack known as the TCP/SYN flood attack to see if using the real server would have a better effect on the network and help reduce the strain that is being placed on the router.

4.2 Experimental Setup

4.2.1 Hardware

Router:

The Juniper J4350 router [28] [69] that was used is one of the J series with 4 fixed Giga Ethernet ports which support gigabit networking, has a built in firewall, uses the OS Junos, and has a built in:

Processor- to run the JUNOS internet software and maintains the routing protocol and routing tables. The processor also create the packet forwarding switch fabric used by the router.

DRAM- provides storage for forwarding tables, routing tables, other routing engine processes, and is used to buffer incoming packets

EPROM- where the serial number of the routing engine is stored.

Crypto Accelerator Module- the cryptographic algorithms that are used by the IPsec (IP security) services, are enhanced by the processor card. The supported algorithms are AES, 3DES, DES, HMAC-MD5, and SHA-1.

Compact flash- the primary storage for microcode, configuration files and software images, which is kept in a slot on the motherboard of the router.

Server:

The server we used is an Apple iMac Pro Server with an Intel Xeon 2.8 GHz quad-core processor, a Broadcom NetXtreme Gigabit Ethernet adapter [15], and 12 GBytes of RAM. The Apple iMac Pro is able to use the Microsoft's "Windows Server Enterprise 2012 R2" operating system [30] [75] [76].

4.2.2 Software

The software used by the Juniper Router is the Junos Software Release [9.2R1.10] (Export edition) Enhanced Services OS, and Microsoft Excel was used to record the collected date form the performance monitor of the router and the simulated web server and create the graphs for the data.

4.3 Parameters of Performance Comparison

In this chapter of the thesis we will be comparing the connection rate of successful connections received by the simulated web server and the CPU Utilization of the Juniper J4350 router.

Connection Rate (connections per second) – This allowed us to keep track of how many connection were created between the simulated server and the simulated clients through the Juniper Router, and monitor the rate of connections per second between the clients and server and record loss of connections due to DDoS attacks.

CPU Utilization- the central processing unit was the second most important parameter to record during the experiments of this chapter. This allowed use to see how the attack traffic was affecting the router and see how the router was able to handle the stress.

CPU User Usage (%) - The router only had an increase in the User Usage when the Real Time Usage showed that almost all of the CPU remaining resources was about to be used, the router would attempt to control the traffic that was going through the network by dropping connections in an attempt to restore the connections being created by the clients. This is recorded in Figures 4.4 and 4.7 in the Results and Discussions Section.

CPU Real Time (%)- The Real Time of the CPU allowed us to record how much of the CPU's resources were being used when the DDoS attacks were being sent, and at what size of the attacks were forcing the CPU to consume most of the resources. This is recorded in Figures 4.3 and 4.6 in the Results and Discussions Section.

4.4 Results and Discussions

4.4.1 Ping Flood Attack

In this experiment we wanted to see if having the firewall active on the server would cause any affect to the networks performance while under an ICMP flood attack, and to do this we replaced the simulated server that we used in chapter two with an Apple iMac Pro server that uses the Microsoft's "Windows Server Enterprise 2012 R2" operating system as shown in Figure 4.1. Then we ran an experiment where we had the ICMP flood attack range from 0 to 1 Gbps

with increments of 0.1 Gbps with random source MAC and IP addresses being sent to the server that had the firewall deactivated called “Real Server no Firewall” and the results were collected in Microsoft Excel which was used to graph the data in Figure 4.2 using the blue bars. Then we repeated the experiment with the firewall activated called “Real Server w/ Firewall” on the server and recorded the data in Figure 4.2 using the orange bars. As we look at Figure 4.2 we can see the comparison of having the firewall active and not active in the server during the experiment, which shows that during the low DDoS attack range from 0 to 40 percent of Gbps having no firewall on the server did better. This lead to the conclusion that there was a chance that maybe the router was intercepting the attack traffic that was trying to pass through the router, and that the reason the connection rate was dropping was that there was a bottle neck being created at the router causing a lot of connections were being dropped. This would mean that the “Real Server no Firewall” simulation was doing better because the firewall was not consuming the servers resources and reducing the connection rate. When the attack range reached 50 % of Gbps the ICMP flood attacks started to reach the server and began to have an effect on the performance of the networks connection rate which shows when having the firewall activated had a better connection rate than not having the firewall activated. Since the experiment “Real Server no Firewall” had the firewall deactivated there was no way for the server to deal with the attack traffic that it was receiving and caused the loss of even more connections on the network. When we look at the attack range from 50% to 90% we can see that the gap in connection rate between the two is slowly shrinking as the attack increases, which shows in the orange bars that the firewall is consuming more of the servers resources in order to prevent the attack traffic from harming the server. At the attack of 90% we can see the both of the simulations have close to the same connection rate, meaning that the attack speed that was

getting to the router was high enough that the firewall was forced to consume enough of the servers resources that it caused the connection rate to drop as low as if it did not have the firewall activated. Then when the attack reached 100% the server was receiving enough of the attack that instead of just dropping the traffic that was entering the server to reduce the strain that is being placed on the server as in the Real Server no Firewall simulation, the firewall kept consuming the servers resources in an attempt to prevent the server from dropping traffic but only ended up making the connection rate even worse.

Next we take a look at how much of the routers resources are being used by checking Figure 4.3 which shows the Real Time Usage of the Juniper routers CPU, and before we event sent any attack traffic through the network we can see that the router is using 76% of its CPU resources. This shows that the traffic being sent from the simulated users to the server already has the router working well over 50%, but when we started sending TCP/SYN flood attack traffic through the router had an average of 90% CPU usage. This means that the router started to show signs of being affected by the attack traffic at a low level even when using the Apple iMac server. As the attack range increased the routers CPU usage slowly increased from a low 90% to a high 90%, but would not reach 100% because this would mean that the router would not be functional. As we look at Figure 4.3 we can see that having the server with the firewall deactivated connected to the network helped improve the network performance during the low attack range 40% bandwidth and lower. In the attack range of 50% to 80% we can see that the server with the firewall activated was doing better out of the two options, and this can be explained as we look in Figure 4.4 which shows that at the attack bandwidth 40% the router started dropping connection in the network with the firewall deactivated which reduced the stress of the router to help the connection rate which was proven when the CPU User Usage increased. When the

attack reached the high range of 90% and up Figure 4.3 shows the network that had the firewall activated was consuming more of the routers resources only, because the network that had the server firewall deactivated was forcing the router to drop more connections and reduce the amount of the routers CPU resources that are being consumed to help protect the network.

Next we will be looking at Figure 4.4 which shows the Juniper routers CPU User usage which represents when the router is being pushed to its limits and is forced to start closing connections of all traffic that is entering the router in an attempt to reduce the strain that the network and attack traffic is placing on the router. This allows the router to reclaim some of the resources that were being consumed due to the attack traffic and explains why as the attack range increased in Figures 4.2 and 4.3 the performance of the two simulation would switch on which was giving better results. In Figure 4.4 we can see that by having the firewall deactivated had the router use the CPU User usage increase at the attack range of 40%, and caused the router to start dropping connection in an attempt to stop the attacks and restore the connections with the simulated server. From the attack range of 50% - 80% the network that had the firewall on the server deactivated and the network that had the firewall on the server deactivated seemed to place the same amount of a strain on the Juniper router until the attack range reached 90% and higher. This is where we see the biggest difference between the two network experimental setup showing that the experiment with the server firewall deactivated was the least favorable for the network by increasing that strain placed on the router by six times than the other network setup. Since the having the firewall deactivated was worse for the performance of the network we decided to leave the firewall activated for the rest of the experiments the will be using the Apple iMac server.

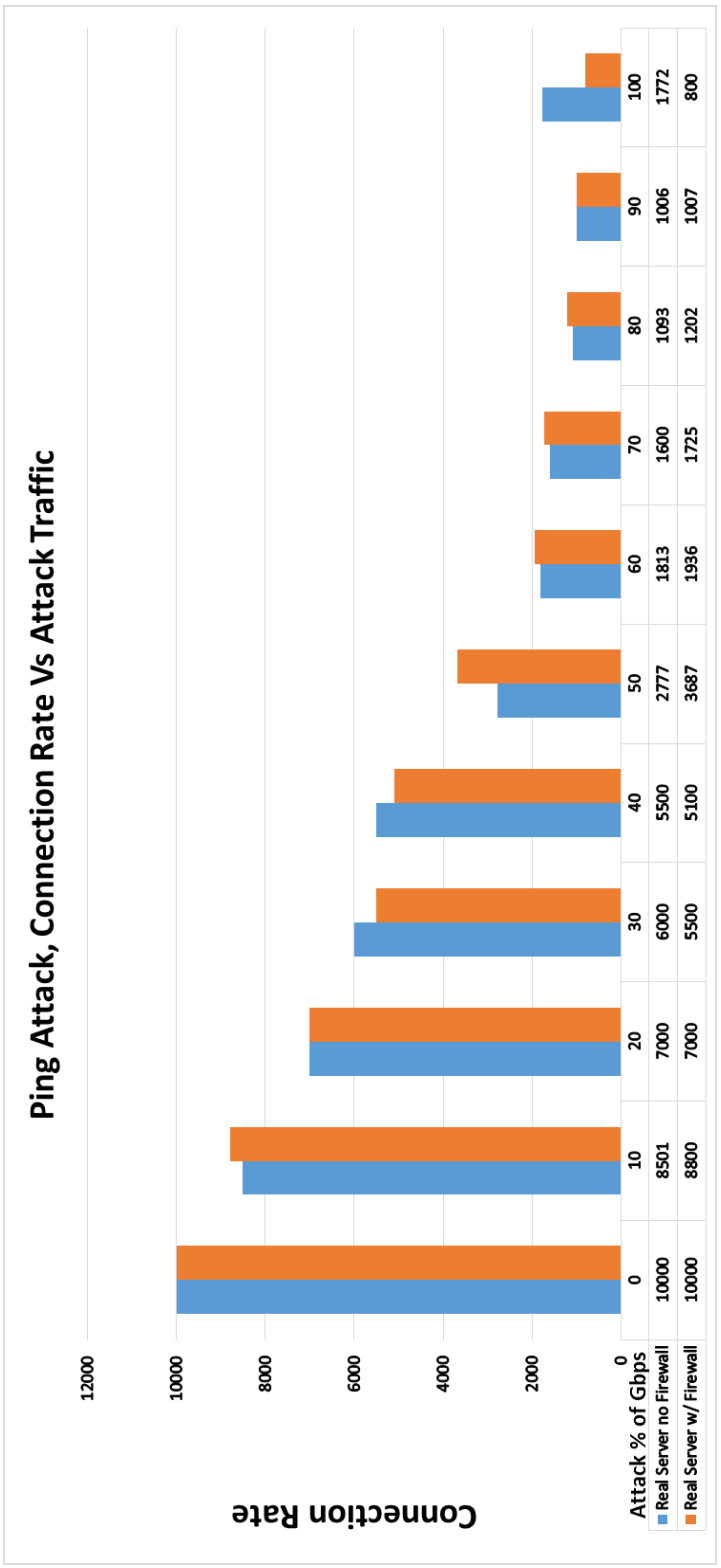

Figure 4.2: Comparison of Firewall Activated and Deactivated Connection Rate

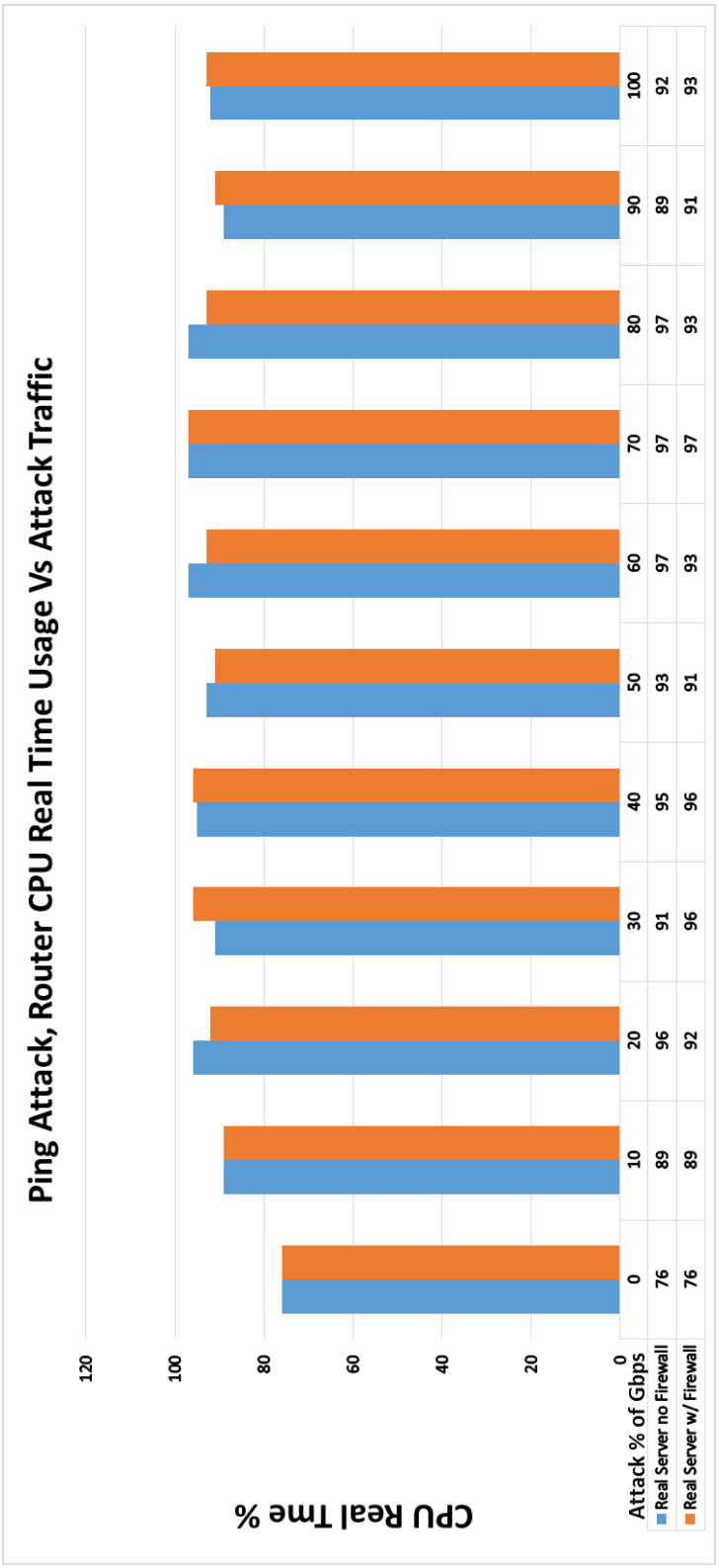

Figure 4.3: Comparison of Firewall Activated and Deactivated CPU Real Time Usage

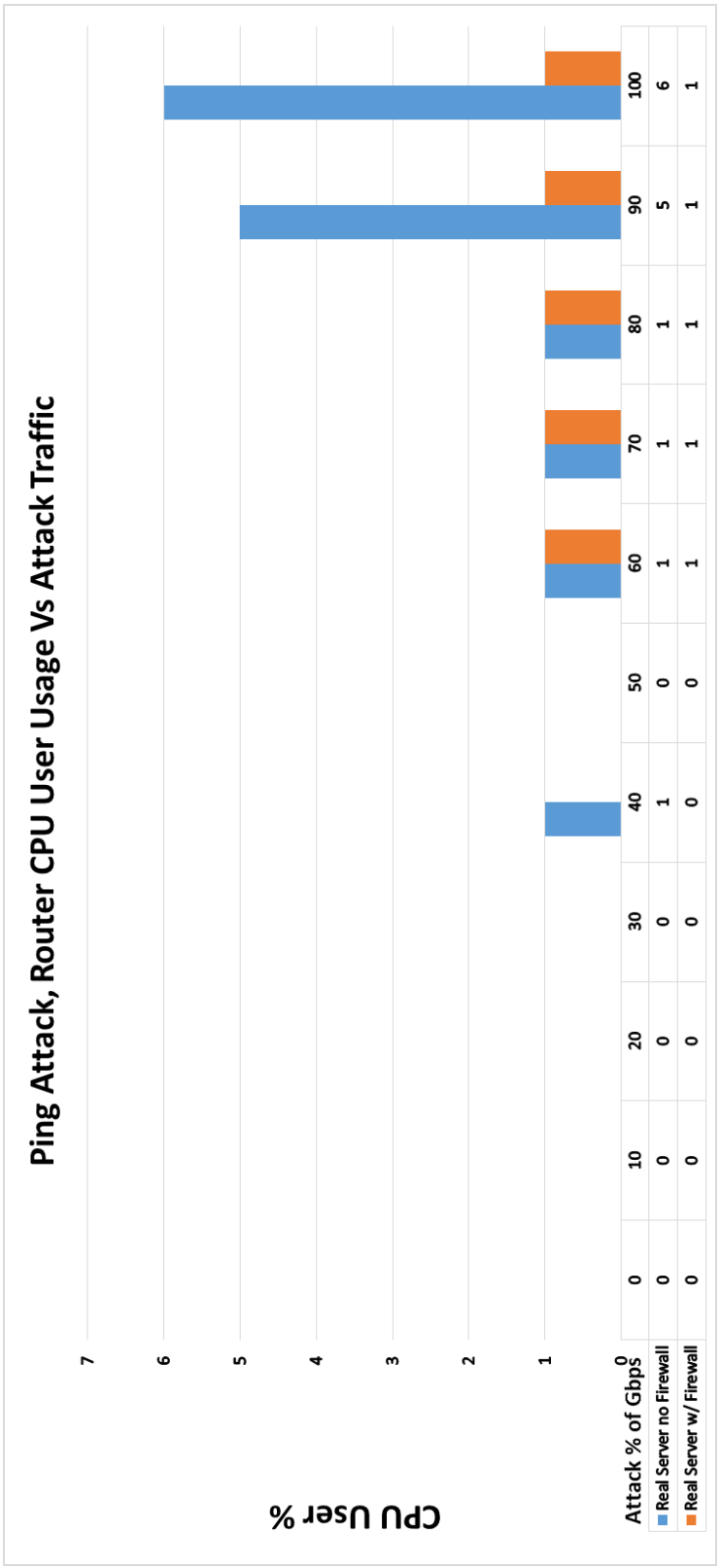

Figure 4.4: Comparison of Firewall Activated and Deactivated CPU User Usage

4.4.2 TCP/SYN Flood Attack

In the previous experiment we found that having the firewall activated on the server help give the best performance for the network compared to having the firewall deactivated on the server. For this experiment we now wanted to see if having the Apple iMac server connected to the network would really help the performance of the network compared to having the simulated server, which does not offer and security or help to the network, connected in place of the real server. In this experiment we wanted to see if having the server with the firewall activated would have a better performance on the networks compared to using a simulated server, and help us get a better understanding if the firewall of the server is really improving the network performance or if the router is dealing with all of the attack traffic. Once again the Default Everything security setting will be placed on the router throughout this experiment to create a controlled testing environment that will not have the router because any affect to the networks performance while a TCP/SYN flood attack is passing through the network. We used the results that we gathered from the network experiment in chapter 3 for the network that used the simulated server and had the Default Everything security setting, while TCP/SYN flood attack was passing through the network and called it simulated server which is represented by the blue bar in Figure 4.5. This network setup was used because the TCP/SYN flood attack had more of an effect on the network than the PING flood attack and the Default Everything is the security setting that we are using in this experimentation. In order to compare the simulated server with the real server we had the Apple iMac Pro server that uses the Microsoft's "Windows Server Enterprise 2012 R2" operating system as demonstrated in Figure 4.1. We also kept the firewall using the Default everything security setting. Then we ran an experiment where we had the TCP/SYN flood attack range from 0 to 1 Gbps with increments of 0.1 Gbps with random source MAC and IP addresses

being sent to the Apple iMac Pro server that had the firewall activated called “Real Server no Firewall” and the results were collected in Microsoft Excel which was used to graph the data in Figure 4.5 using the red bars. As we look at Figure 4.5 we can see the comparison of having the Apple iMac Pro server with the firewall active “Real Server with Firewall” on the network and having the simulated server attached to the network. In Figure 4.5 we can see that when the attack range was low and below 30% of the attack bandwidth the simulated server helped the network to have a better connection rate than the network that used the Apple server. As the attack bandwidth increased from 10% to 20% the gap in the difference between the connection rates started to drop until the attack range reached 30%, which mean that maybe the router was able to prevent the attack traffic from reaching the servers in exchange for reducing the connection rate. Then that would mean that the reason the network with the Apple server has a lower performance is because the software on the server is consuming the servers CPU resources which is also affecting the connection rate of the network. The performance between the two networks switch when the attack bandwidth reached 30% which had the network with the Apple server helping the performance of the network, which also means that some of the attack traffic was starting to get past the router and reaching the servers. Since the simulated server has to protection against the TCP/SYN flood attack it was affected the most and dropped more connections at the server side of the network causing the performance of the network to fall more. This continued for the attack range of 30% to 90%, and as the attack bandwidth kept increasing more of the attack traffic kept passing through the router and reaching the servers. While attack range increased more and more TCP/SYN flood attack kept reaching the Apple server with the firewall, and the more the firewall worked to protect the connections and stop the DDoS attacks from harming the server. This resulted in the consumption of the Apple server’s

CPU resources which then lowered the number of connections that can be established with the server, and caused the gap in the connection rate between the two networks to slowly close. When the attack range reach 90% there was barely a difference of 100 connections per second which did not show much of a difference between the two servers used in this experiment. After the attack range reached 100% the firewall of the Apple server still refused to give up on dropping the connections to reduce the strain that was being placed on the server, and consumed more of the servers CPU resourced causing the connection rate of the network to drop below the connection rate of the network that used the simulated server.

Next we take a look at the at the CPU consumption of the router that is being caused during the DDoS attack when we had the servers connected to the network which is represented in Figure 4.6 which show the Juniper routers CPU Real Time Usage. In Figure 4.6 we can see that the network that used the Apple server helped to reduce the strain that was placed on the Juniper router since the Real Time Usage had an average of 60% while the network that used the simulated server had a Real Time Usage close to 90% throughout the experiment. This showed that even if the connection rate for both networks was close during the TCP/SYN flood attack the network that puts less of a strain on the Juniper routers CPU would be the best option. In order to make sure that the low CPU Real Time Usage was because the router was connected to the network we have to compare the CPU User Usage of the two networks in Figure 4.7 to see if the low Real Time Usage was not caused by the router increase in the CPU User Usage in an attempt to drop connections and reduce the strain on itself. In Figure 4.7 we can see that the network that used the simulated network put the most strain on the router causing it to use the CPU User Usage at a low attack bandwidth of 30%, which means the router started to drop connection to reduce the amount of CPU resources that was being consumed by the router. Since the network

that used the Apple iMac Pro Server did not force the Juniper router to use the CPU User Usage until the attack range reached 60%, that means in Figure 4.6 the low use of the CPU Real Time Usage was thanks to the help from the Apple server. The use of the Apple iMac Pro server with the firewall activated not only helped to improve the connection rate, but also helped to reduce the strain on the router compared to using the simulated server on the network.

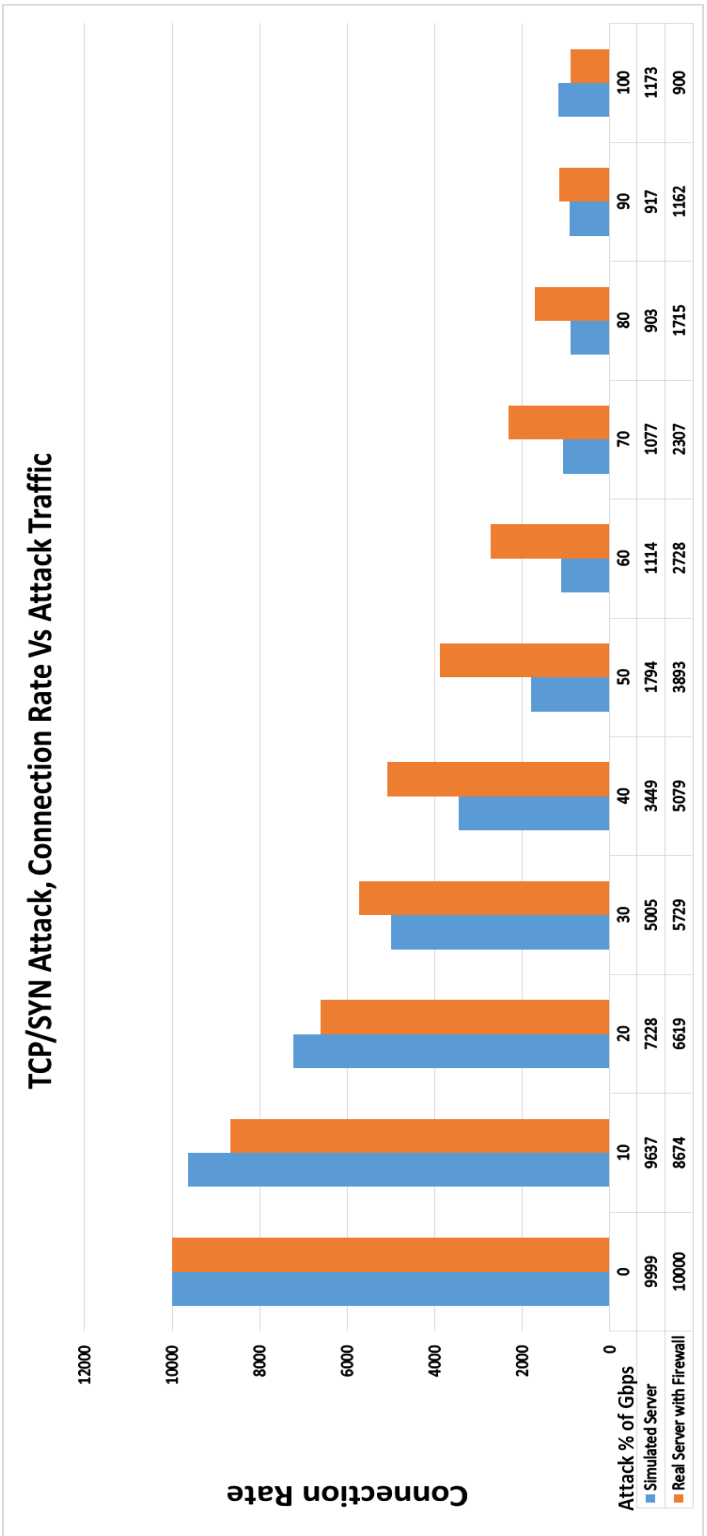

Figure 4.5: Comparison of Simulated Server vs Real Server with Firewall Connection Rate

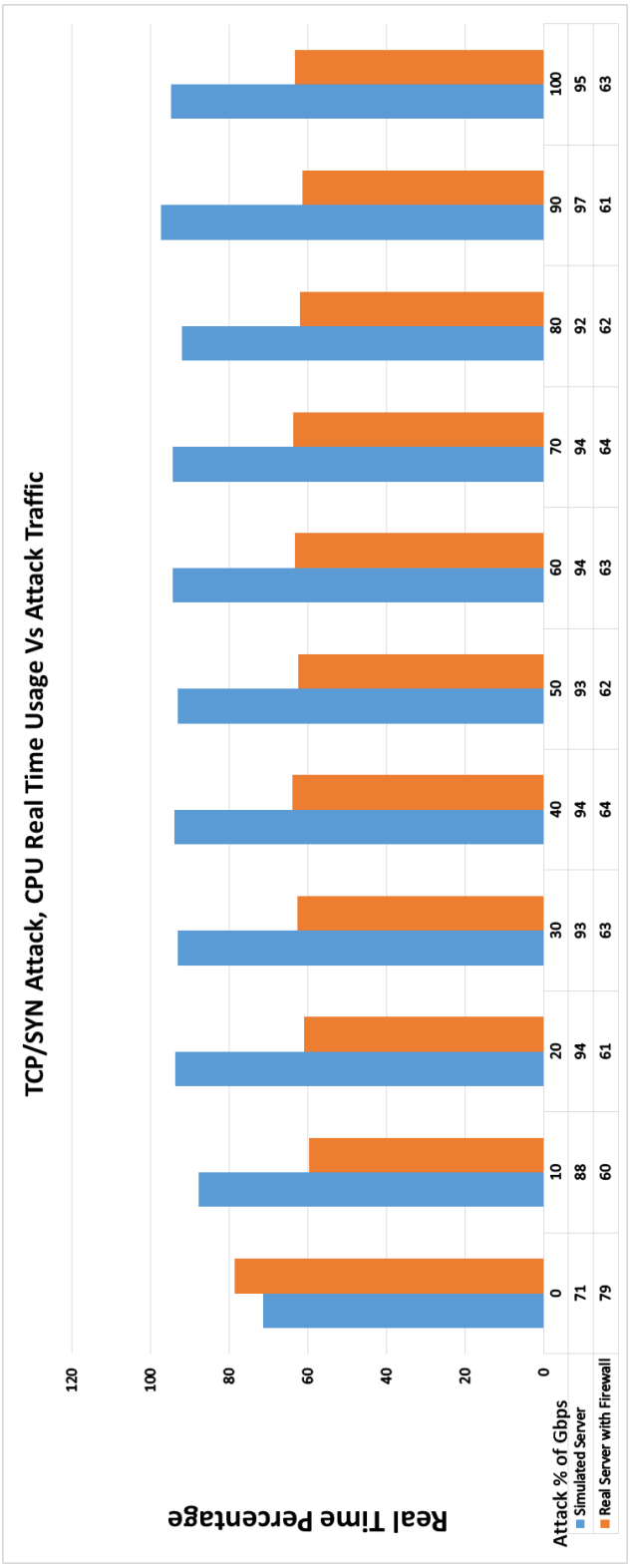

Figure 4.6: Comparison of Simulated Server vs Real Server with Firewall CPU Real Time Usage

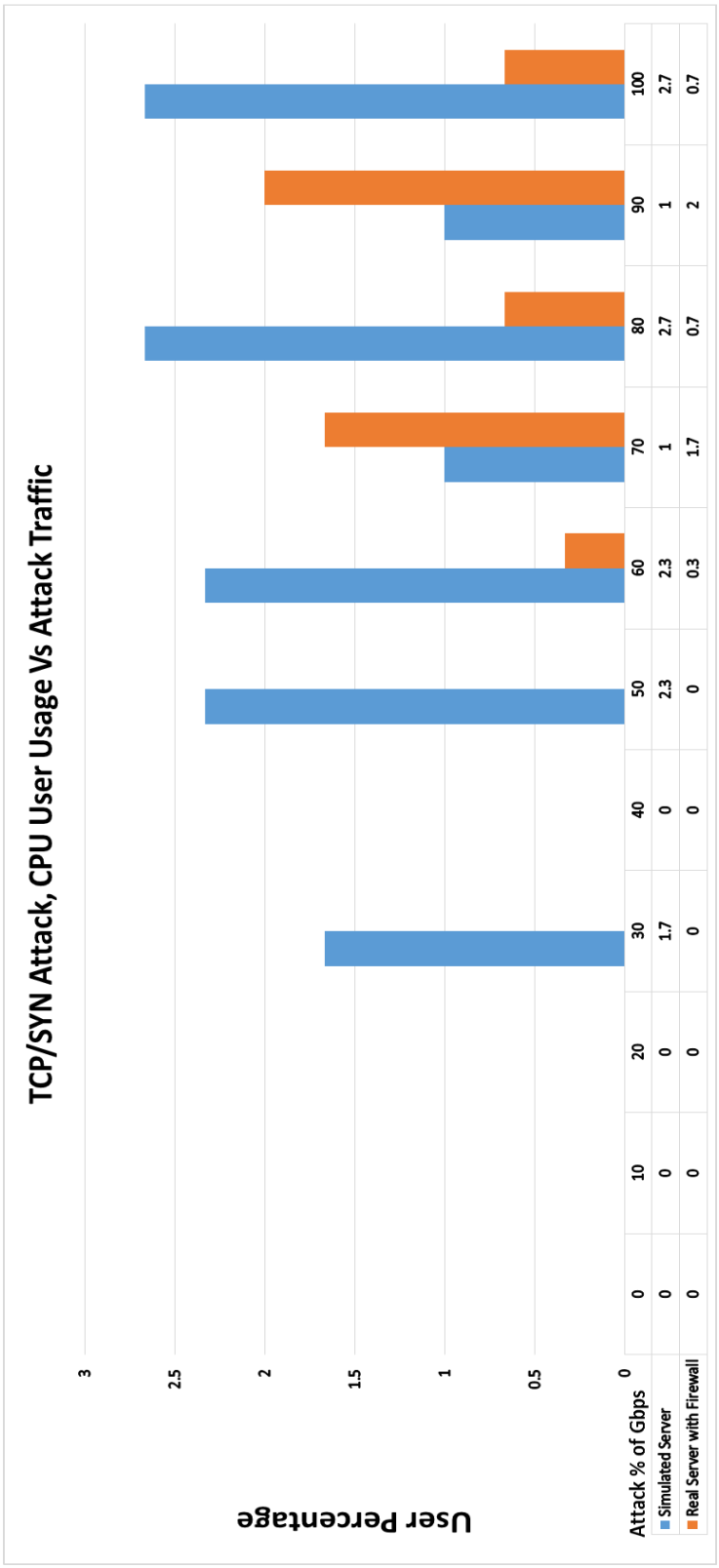

Figure 4.7: Comparison of Simulated Server vs Real Server with Firewall CPU User Usage

4.5 Chapter Summery

We reviewed the results that were obtained from the ICMP echo request flood attack experiments that we tested in this chapter to compare the effects on the networks performance with having the firewall activated and deactivated on the Apple iMac Pro server that was configure with the Microsoft "Windows Server Enterprise 2012 R2" operating system. We configure the Juniper J4350 routers firewall to use the Default Everything security setting that we used in chapter three for all the experiments in this chapter which would mean that any changes in the network performance would be caused by any changes in the server. The results proved that having the firewall activated not only improved the connection rate of the network, but also put less of a strain on the router by helping it use less of the routers CPU resources. In the next experiment we wanted to see if using the Apple iMac Pro Server with the firewall activated was really helping the network by comparing the server to the simulated server that we used in chapter 3. For the experiment we configured the router to use the Default Everything security setting that we used in the previous experiment and had the simulated attackers send TCP/SYN flood attack through the network to the server while first having to pass through the Juniper Router. When we compared the results of the network that used the simulated server and the network using the Apple iMac Pro server with the firewall activated, we found that having the Apple server helped improve the performance of the network and helped reduce the amount of resources consumed by the router CPU. This showed that the firewall from the Apple iMac Pro server helped improve the network performance while under DDoS attack. One of the problem that we still need to take a look in is that even though the changes we make to the network have had different effect on the performance of the network the connection rate would

still drop. When the connection rate would reach 100% attack bandwidth for either the ICMP echo request flood attack or the TCP/SYN flood attack the connection rate dropped from 10,000 connections per second to close to 1,000 connections per second.

CHAPTER V

COMPARISON OF NETWORK PERFORMANCE UNDER SECURITY ATTACKS USING SIMULATED SERVER, A SERVER WITH MICROSOFT'S WINDOWS 2012 ENTERPRISE R2, AND SERVER WITHOUT ROUTER.

5.1 Introduction

For the experiment, we configured the Juniper J4350 router with Junos Software Release [9.2R1.10] (Export edition) Enhanced Services OS Junos in a star topology network as seen in Figure 5.1 and 5.2, and used Category 6 Ethernet cables to connect all the network devices.

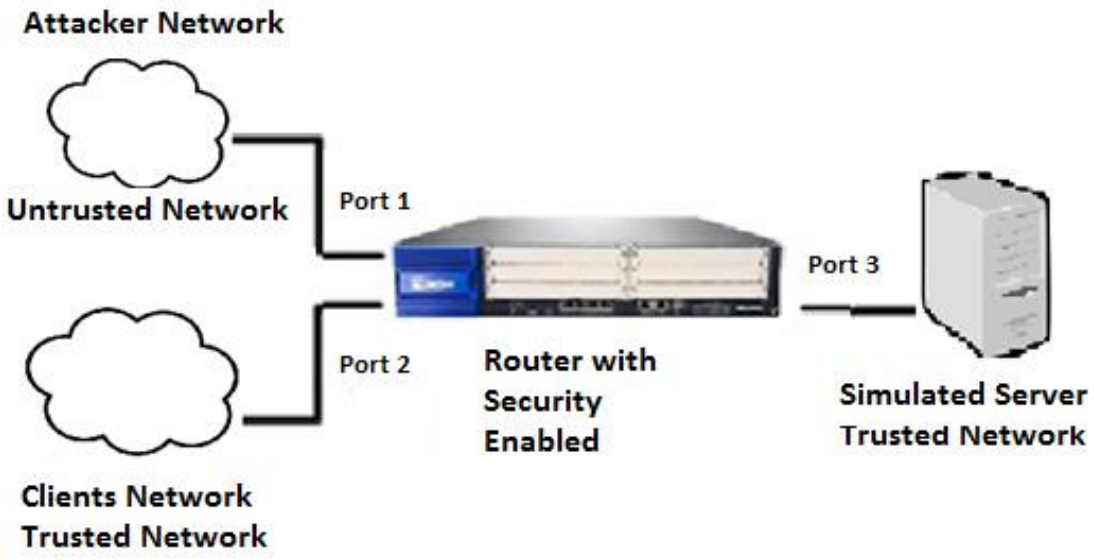

Figure 5.1: Experimental Setup for Router with simulated server.

We first started by using [29] [58] - [62] to help us configure the router to be able to interact with the networks that we wanted to work with as shown in Figure 5.1 & 5.2. Since the router was able to have the firewall act as a Stateless or a Stateful firewall, we chose to configure the router as a Stateful since that is one of the most common firewall configuration used today.

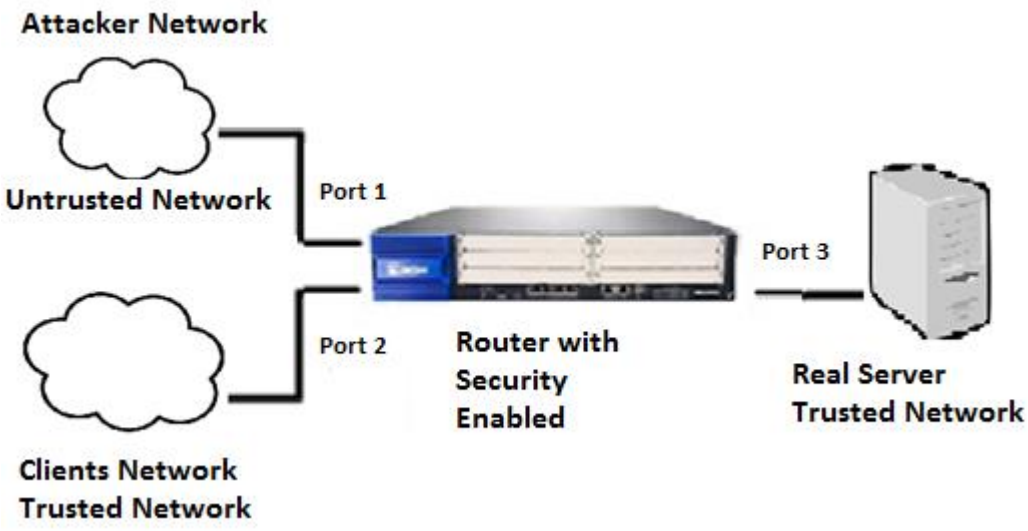

Figure 5.2: Experimental Setup for Router with Real Server.

This allowed the router to use flow base forwarding and worked more in handling with the connections that are going through the router instead of monitoring every packet. Having the router in Stateful allowed us to create trusted and untrusted zones and configure policies that will control how different zones interact with each other. The Juniper J4350 is able to handle up to 1 Gigabyte per Second of traffic at each port which is why we used two networks to simulate TCP/SYN attack on the 192.168.1.0/24 network and had it placed as untrusted networks, while we kept 192.168.2.0/24 and 192.168.3.0/24 networks on the trusted zone. The attacking network were placed on different network to allow us to simulate TCP/SYN traffic that would use random source IP addresses and MAC addresses within the range of the network, so that there

will not be any collisions between the legitimate traffic from the clients and the attack traffic from the attackers, and use a more real world TCP/SYN flood attack traffic which will make it even harder for the router to stop the attack.

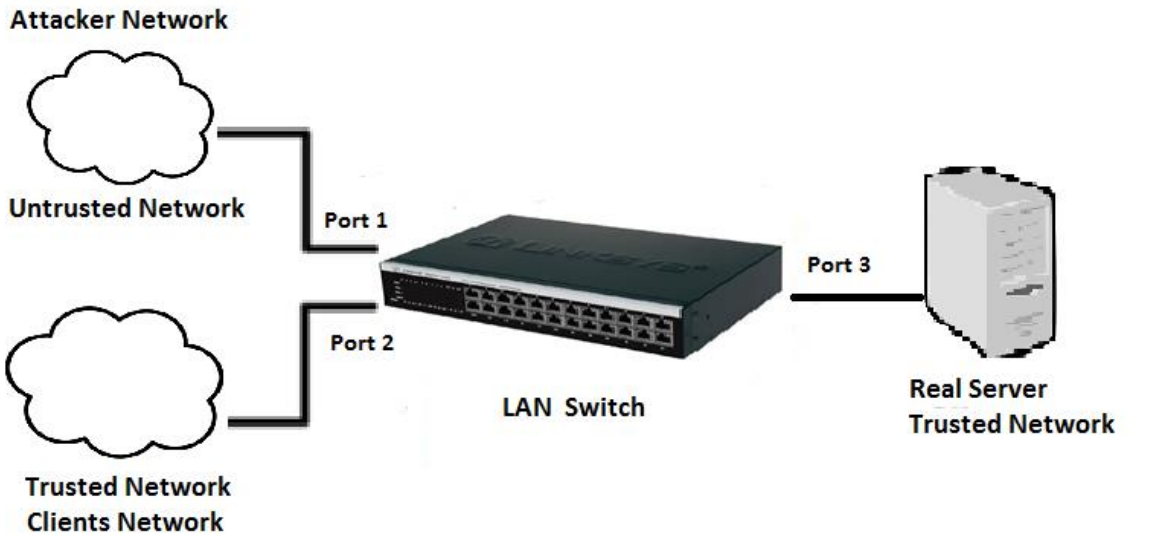

Figure 5.3: Experimental Setup for Real Server without router.

Next we configured a simulated server and an Apple iMac Pro Server with an Intel Xenon 2.8 GHz quad-core processor with a 12 GBytes of RAM using the operating system Microsoft "Windows Server Enterprise 2012 R2" server on network 192.168.3.0/24 and be switched between the two too work as a web server that will allow us to use http traffic, and the legitimate users on network 192.168.2.0/24 would use the GET command to retrieve a 1 bite web page from the server. Using the smallest size web page allowed the router to handle a higher connection rate, which was 10,000 Connections per Second. Together the attack networks were used to create TCP/SYN flood attack that ranged from 0 to 1,000 Mbps with increments of 100 Mbps with random source IP addresses and was sent to the server on network 192.168.3.0/24 with an IP address of 192.168.3.2. For the first test used in the experiment we started with using

a simulated server without having a firewall active, which would leave the router with the only form of security on the network to prevent the DDoS attacks from reaching the simulated server. In the second test that we performed the simulated router was replaced with the Apple iMac Pro Server with an Intel Xenon 2.8 GHz quad-core processor with a 12 GBytes of RAM using the operating system Microsoft "Windows Server Enterprise 2012 R2" server which had the firewall and repeated the first test. In the third experiment we kept the Apple iMac Pro Server in the network and replaced the Juniper J4350 router with the Cisco SRW2024 24-port Gigabit Switch. This allowed us to see how much of the connection loss was happening from the server side of the network during the DDoS attacks and allow us to compare the three sets of results and see how the router affected the network.

5.2 Experimental Setup

5.2.1 Hardware

Router:

The Juniper J4350 router [28] [69] that was used is one of the J series with 4 fixed Giga Ethernet ports which support gigabit networking, has a built in firewall, uses the OS Junos, and has a built in:

Processor- to run the JUNOS internet software and maintains the routing protocol and routing tables. The processor also create the packet forwarding switch fabric used by the router.

DRAM- provides storage for forwarding tables, routing tables, other routing engine processes, and is used to buffer incoming packets

EPROM- where the serial number of the routing engine is stored.

Crypto Accelerator Module- the cryptographic algorithms that are used by the IPsec (IP security) services, are enhanced by the processor card. The supported algorithms are AES, 3DES, DES, HMAC-MD5, and SHA-1.

Compact flash- the primary storage for microcode, configuration files and software images, which is kept in a slot on the motherboard of the router.

Server:

The server we used is an Apple iMac Pro Server with an Intel Xeon 2.8 GHz quad-core processor, a Broadcom NetXtreme Gigabit Ethernet adapter [15], and 12 GBytes of RAM. The Apple iMac Pro is able to use the Microsoft's "Windows Server Enterprise 2012 R2" operating system.

Switch:

We used the Cisco Linksys SRW2024 24- port Gigabit Switch to help us connect all of the Simulated users to help make it easier to send all of the traffic from the simulated users to go through the port on the router which is meant for the network that is to communicate with the simulated users. The Cisco SRW2024 switch can handle 24 Ethernet connection that can each handle Gigabit networks which can be found in [31] [77].

5.2.2 Software

The software used by the Juniper Router is the Junos Software Release [9.2R1.10] (Export edition) Enhanced Services OS, and Microsoft Excel was used to record the collected date form

the performance monitor of the router and the simulated web server and create the graphs for the data.

5.3 Parameters of Performance Comparison

In this chapter of the thesis we will be comparing the connection rate of successful connections established between the simulated clients and the servers on the other end of the network. The data is then recorded on Windows Microsoft Excel 2013 and then graphed the results of the data.

5.4 Results and Discussions

In most cases when using a network for major companies or for your own personal use, one of the main things that comes to a person's mind is which part of the network is the weakest link that hackers try to take advantage of when trying to hack a network. In the past hackers would direct their attack to the computer or server that they wanted to take down using Denial of Service attacks. When people started to use firewall software to detect and stop the DoS attack, hackers started to use Distributed Denial of Service attack to make it harder for victims to detect the attacks and stop the attacks. One of the problems that occurred when putting stronger security software on the computer and server was that a lot of resources needed to be used to run the security software on the server and computer. Many people would just increase the resources that were available in the server and computer which also increased the cost of the devices, but some companies decided to distribute firewall software to other devices that are used in the network such as the router. Doing this allowed companies to increase security of the overall network without having to put all of the strain on the server and computers. In this paper we

plan on showing if having the extra security on a Juniper J4350 Router would be beneficial for the network.

As we look at Figure 4 in section 3 experiment setup we can see the first experiment setup for this paper, and the purpose of this experiment setup was to get a better understanding of what the security of the Juniper router offered for the network without having security features that are always on in a real server interfering with our data results. The data was then collected and then recorded in Figure 7 represented in the yellow color bars and we can see how the Juniper router with a built in firewall affected the connection rate of the network that had traffic for the simulated clients and the TCP/SYN flood attack at the different sizes of the DDoS attacks as the attacks incremented by 10% of a Gigabyte size attack. When the data was collected we replaced the simulated server in the network with an Apple iMac Pro Server with a single processor Intel Xenon 2.8 GHz quad-core processor, and had a 12 Giga Bytes of RAM. The server was compatible with the operating system Microsoft "Windows Server Enterprise 2012 R2", and as explained in section 3 the firewall was enabled since in most cases the firewall is already enabled on the devices. We repeated the same experiment the was done on the simulated server for a real server with router using the same increment of the TCP/SYN flood attack and recorded the data on Figure 6 using the blue bars. As we compare the yellow and blue bars that represent the networks connection rate we can see that when the TCP/SYN flood attack rate was below 30% of a 1 Giga Bite per second the simulated web server that was used without a firewall did better than the real server with router with the Windows firewall active. Even though the connection rate was better when the destination was the simulated server, the connection rate was only better by nearly 1000 connections per second which showed that for the small attacks the router was dealing with the attack traffic going through the network which lowered the connection rate

without the servers knowing that there was attack traffic trying to reach the server. When the attack rate reached 30% and above that the Juniper router started to show signs that the router could not prevent all of the attack traffic from passing through the router because the simulated server began to have a lower connection rate than the real server with the active firewall. As we look at Figure 7 we can see that the servers started to receive some of the TCP/SYN attack traffic, because the simulated server started to have a lower connection rate than the real server with router which means that the firewall on the real server with router started to work on preventing the DDoS attack from causing harm to the connection rate while the simulated server which had no firewall was losing more connections.

While the attack percentage increases we can notice that the difference between the simulated server and real server with router is created by the difference of having a firewall on or off, but the connection of the real server with router, which is higher than the both, is still dropping which show that the router is dropping more of the connections from the simulated clients in an attempt to prevent more attack traffic from reaching the server. In order to show that most of the connection loss was happening at the router, we ran the third experiment explained in section 3. In this experiment we removed the router from the network and had the router replaced with a Cisco SRW2024 24-port Gigabit Switch that has no firewall, this would allow the simulated clients traffic and the DDoS attack to reach the real server with the firewall enabled and see how the firewall of the real server without router was helping the server and the data was recorded in Figure 6 represented by the orange bars. In Figure 7 we can see that when the DDoS attack rate was between 0% and 90% the real servers firewall prevented the DDoS attack from having too much of a loss of the connection rate, which show that the connection rate shown for the real server with router for the range of 0% to 90% of the DDoS attack was caused

by the router. When the DDoS attack reach 100% or 1 Giga Bite per second of attack enough of the TCP/SYN flood attack was too much for the servers firewall to handle and the connection rate began to fall.

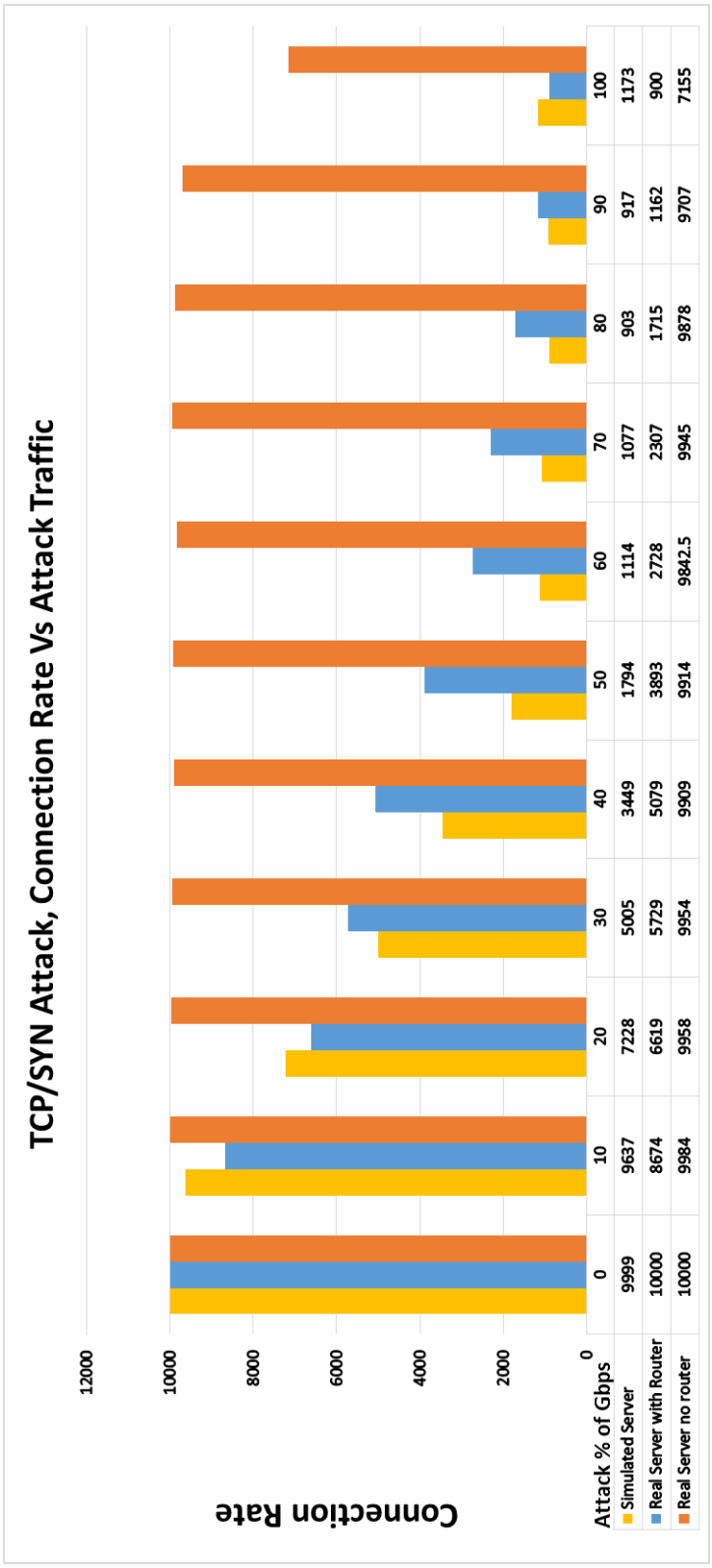

Figure 5.4: Simulated Server vs Real Server vs Real Server with No Router

5.5 Chapter Summery

As we review the results that we gained from the TCP/SYN Flood attack experiments that were simulated in this thesis to test the limitations of the router by using a simulated clients, simulated server, a real server and a real server without router. After all the testing and collection of the data on the number on the connection rate of the network between the server and clients we were able to see that when we look at the connection rate we were able to see the how much the firewall from the real server was able to improve the connection rate of the network and by how much it was improving the connection rate of the network. We were able to see how most of the connection that were lost was happening at the router, and this became clear when we removed the router with a Cisco SRW2024 Gigabit Switch with 24-port and saw that the real server was not affected much by the DDoS attack. This showed that even though the router had a built in operating system and firewall, the router ended up dropping good connections in order to prevent DDoS attack traffic from reaching the server.

CHAPTER VI

CONCLUSION

Over the years networking companies like Juniper have been working on increasing network security by placing firewalls on their networking devices such routers in an attempt to spread the network security throughout the network. This was to help prevent the need of having security protection features confined only to servers and computers. More security that was placed at the endpoints of the network the more CPU resources were consumed, which lowered the performance of the servers and computers. The Juniper J4350 router with Junos Software Release [9.2R1.10] (Export edition) came with built in firewall which the company said could handle a connection rate of 10,000 connections per second.

In this thesis the Juniper J4350 router with Junos Software Release [9.2R1.10] (Export edition) Enhanced Services OS Junos with built in firewall was evaluated to see if the router was able to help improve the security of a network as the Juniper Company claimed. We examined how two of the most common DDoS attacks, the ICMP echo request flood attack and the TCP/SYN flood attack, would influence the router's security and network performance. The firewall was configure to use four of the most common security settings that would work with a firewall such as the NO Security, NO Ping Through, Default, and Default Everything and how they helped the router.

We reviewed the results gained from the ICMP Flood and the TCP/SYN Flood attack experiments that used simulated clients and server. The data form the router and the server, allowed us to see that the connection rate did not show much of a difference in the drop of the connection rate from the different security setting used on the router. Then we examined at how much of a strain that the DDoS attacks were putting on the router by observing the CPU User Usage we were able to see that there was a much greater difference on how the different security setting had on the router. During the ICMP flood attack the results showed that using the Default security setting forced the router to be pushed to its limits at only 100Mbps, as was followed by the security setting that prevented the ICMP packets from passing through the router which caused the router to use the CPU User Usage when the attack reached 200Mbps. This showed that these two would be the least affective in helping to protect the network during a DDoS ICMP flood attack, while the Default Everything and the No Security did a little better even though the loss in the connection rate was nearly similar to the other two during the lower half of the attack range. We discovered that in Figure 3.6 the No Security, Default and Default Everything security settings also did not have much of a difference when protecting the connection rate in the network. Figure 3.8 allowed us to understand the differences of the three security setting which showed that the NO Security setting ended up putting more of a strain on the router by forcing the router to use up more CPU resources and drop connection at an attack of 10% of the 1Gbps. The Default Everything security setting was second in pushing the router to use the routers CPU User Usage at an attack of 30% of the 1Gbps, which meant that the security setting Default was able to help protect the network with the same efficiency as the other two and put the less strain on the router.

Next we compared the effects on the performance between having the firewall activated and deactivated on the Apple iMac Pro server that was configure with the Microsoft "Windows Server Enterprise 2012 R2" operating system. The Juniper J4350 routers firewall was configured to use the Default Everything security setting for the rest of the experiments which would mean that any changes in the network performance would be caused by any changes in the server. The data gathered showed that the firewall activated improved the connection rate of the network, and put less of a strain on the router by reducing the routers CPU resource consumption. In the next experiment we wanted to see if using the Apple iMac Pro Server with the firewall activated helped the network by comparing the Apple server to the simulated server. Then we configured the router with the Default Everything security setting that was used in the previous experiment and sent TCP/SYN flood attack through the network to the server which first had to go through the Juniper Router. We compared the performance of both networks, and the results showed that the Apple server helped improve the performance of the network and reduce resources consumption by the router CPU. The results showed that the firewall from the Apple iMac Pro server helped improve the network performance while under TCP/SYN flood attack. This still left us with a problem that we still need to look into is even though the changes made to the network had different effect on the performance of the network still dropped. After the connection rate would reach 100% attack bandwidth for either the ICMP echo request flood attack or the TCP/SYN flood attack the connection rate fell from 10,000 connections per second to nearly 1,000 connections per second.

Collection of the data on the number on the connection rate of the network between the server and clients reveled that when we look at the connection rate the firewall from the real server was able to improve the connection rate of the network and by how much it was

improving the performance of the network. We saw how most of the connection that were lost was happening at the router, and this became clear when we replaced the router with a Cisco SRW2024 Gigabit Switch with 24-port and observed that the real server was unaffected by much of the TCP/SYN flood attack. This showed that even though the router had a built in operating system and firewall, the router dropped good connections in order to prevent DDoS attack traffic from reaching the server.

When the router was connected to the network using the Default Everything security setting, the router had to perform extensive checks on all the connections to prevent any form of attack that might pass through the router. The connection rate of the network to determine the performance of the network and noticed that the performance of the network started to decline at a low attack bandwidth of 10 Mbps. After the attack range reached to 90 Mbps the connection rate was reduced to nearly 1162 connections per second out of the 10,000 cps suggested by the company Juniper. The Juniper J4350 router with the firewall activated the router ended up becoming a bottleneck within the network when DDoS traffic was passing through the router.

After we replaced the router with the Cisco Linksys SRW2024 with 24-port Gigabit Switch the Apple server with the firewall activated was left as the only device with security against DDoS attacks. This meant that the server had to protect itself from the TCP/SYN flood attacks. The server was able to support the 10,000 connection while being targeted by the DDoS attack, until the attack bandwidth reached 90 Mbps which was when the connection rate dropped from 10,000 cps to 7155 cps.

Even though the Juniper company data sheet claimed that the Juniper J4350 router could support 10,000 connects in a network. The router was only able to support close to 900 cps while the network was under a high bandwidth DDoS attack. The router with a built in firewall

and security protection did not improve the performance of the network, instead the router lowered the connection rate of the network. This is why network companies need to properly test their devices, otherwise the extra security that they are placing on their device could be the cause of the degradation of the network performance.

REFERENCES

[1] S. Prell, Extra Life charity comes under DDoS Attack, *Endgadget*, 11/02/13. Last Access on DEC-09, 2016 http://www.joystiq.com/2013/11/02/extra-life-charity-comes-under-ddos-attack/

[2] (2013). DDoS Attacks Against Government and Entertainment Websites Escalate; *Infosec Island*. last Access on DEC-09, 2016 http://www.infosecisland.com/blogview/19543-DDoS-Attacks-Against-Government-and-Entertainment-Websites-Escalate.html

[3] Franzen, Carl (2013) 'Largest' public denial of service attack in internet history linked to Europe span dispute. *The Verge*.

[4] Westervelt, Robert (2013). DDoS Attack Behind Latest Network Solutions Outage. *CRN*. last Access on DEC-09, 2016 http://www.crn.com/news/security/240158492/ddos-attack-behind-latest-network-solutions-outage.htm

[5] Julianne Pepitone. (2013). Hackers Mount Denial-of-Service Attack With Computer Clock Tool, *NBC News*.

[6] Dan Goodin (2014). New DoS attacks taking down game sites deliver crippling 100Gbps floods. *ARS Technica*.

[7] (2002). NETWORK PROTOCOL FIREWALLS/ROUTERS NOT ADEQUATE FOR XML Computer Protocols15.9. last Access on DEC-09, 2016 http://search.proquest.com/docview/202828674?pq-origsite=summon

[8] Richard Karpinski (2002). Study: Routers, Firewalls Can't Handle XML Traffic; New class of devices not only understand network protocols, but the contents of the XML documents that travel over them, *InternetWeek*.

[9] F.A. El-Moussa, N. Linge, and M. Hope (2007). - Active router approach to defeating denial-of-service attacks in networks, communications, *IET* Volume 1, Issue 1, Page(s):55-63

[10] Yau, D.K.Y., Lui, J.C.S., Feng, L., and Yeung, Y, (2005). -Defending against distributed Denial of service attacks with max-min fair server-centric router throttles, *IEEE/ACM Trans. Netw*. 13, (1), pp. 29-42.

[11] (1996). Bay Building Firewalls into Routers Semilof, Margie. *CommunicationsWeek* : 01.

[12] (1997). "Cisco adds firewall to new router." *Web Week*, p. 29. General OneFile.

[13] Jeff Wilson (2004). Enemy at the gates: the evolution of network security; Lights, camera, action! Firewalls, appliances and routers take center stage in the never-ending battle for network security, *Business Communications Review*. 34.12: p14.

[14] Salamone, Salvatore (1997). Securing The Branch Office -- Cisco offers low-cost access router, new software-based firewall. Phillips *Business Information's Internet Week* 687: PG8.

[15] Jeff Wilson (2005). The future of the firewall: security functions are finding new homes in appliances, switches and routers, *Business Communications Review*. 35.5: p28

[16] Linge, N; Hope, M (2007). Active router approach to defeating denial-of-service attacks in networks, El-Moussa, F A; *IET Communications1.1*: 55-63.

[17] T. Katic, M. Sikic and K. Sikic (2005). "Protecting and controlling virtual LANs by Linux router-firewall," *27th International Conference on Information Technology Interfaces*, pp. 518-523. doi: 10.1109/ITI.2005.1491182

[18] G. Attebury and B. Ramamurthy (2006). "Router and Firewall Redundancy with OpenBSD and CARP," *2006 IEEE International Conference on Communications, Istanbul*, pp. 146-151. doi:10.1109/ICC.2006.254719

[19] Young-Ho Kim and Jeong-Nyeo Kim (2005) "Design of firewall in router using network processor," *The 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005., Phoenix Park*, pp. 658-660. doi: 10.1109/ICACT.2005.245955

[20] Lili Qiu, G. Varghese and S. Suri (2001). "Fast firewall implementations for software and hardware-based routers," *Proceedings Ninth International Conference on Network Protocols. ICNP 2001*, pp. 241-250. doi: 10.1109/ICNP.2001.992904

[21] F. N. Ugwoke, K. C. Okafor and V. C. Chijindu (2005). "Security QoS profiling against cyber terrorism in airport network systems," *2015 International Conference on Cyberspace (CYBER-Abuja), Abuja*, pp. 241-251. doi: 10.1109/CYBER-Abuja.2015.7360516

[22] M. Singhal (2000). "Security mechanisms in high-speed networks," *Proceedings Ninth International Conference on Computer Communications and Networks (Cat.No.00EX440)*, Las Vegas, NV, pp. 482-. doi: 10.1109/ICCCN.2000.885533

[23] F. Han, L. Xu, X. Yu, Z. Tari, Y. Feng and J. Hu (2016). "Sliding-mode observers for real-time DDoS detection," *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, Hefei, pp. 825-830. doi: 10.1109/ICIEA.2016.7603695

[24] K. Kaur, S. Kaur and V. Gupta (2016) "Software Defined networking based routing firewall," *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, New Delhi, pp. 267-269.doi: 10.1109/ICCTICT.2016.7514590

[25] C. Lévy-Leduc (2008). "Detection of network anomalies using rank tests," *2008 16th European Signal Processing Conference*, Lausanne, 2008, pp. 1-5.

[26] N. A. Noureldien and M. O. Hussein (2009). "Block Spoofed Packets at Source (BSPS): A method for detecting and preventing all types of spoofed source IP packets and SYN flooding packets at source: A theoretical framework," *2009 Second International Conference on the Applications of Digital Information and Web Technologies*, London, pp. 579-583.doi: 10.1109/ICADIWT.2009.5273927

[27] Junper Networks, Juniper Network J-Series Services Routers: J2320, J2350, J4350, and J6350. last Access on DEC-09, 2016 file:///C:/Users/User/Downloads/juniper_j_series.pdf

[28] Website of Juniper J4350 Router Datasheet. last Access on DEC-09, 2016 https://www.juniper.net/techpubs/hardware/junos-jseries/junos-jseries96/junos-jseries-hardware-guide/index.html?hw-hardware-features-j4350-j6350.html

[29] JUNOS® Software Security Configuration Guide. last Access on DEC-09, 2016. available online at http://www.juniper.net/techpubs/software/junos-security/junos-security10.1/junos-security-swconfig-security/junos-security-swconfig-security.pdf

[30] Windows Server 2012 R2. last Access on DEC-09, 2016 http://www.mmicrosoft.com/en-us/server-cloud/products/windows-server-2012-r2/explore.aspx

[31] Website of datasheet for Cisco SRW2024 24-port Gigabit Switch. last Access on DEC-09, 2016 http://www.cisco.com/en/US/products/ps9989/index.html

[32] Networking Computing, Juniper, Cisco Hardware Vulnerable To DoS Attacks. last Access on DEC-09, 2016 http://www.networkcomputing.com/networking/juniper-cisco-hardware-vulnerable-dos-attacks/478224577

[33] Tom Spring (2016)., Juniper Hotfixes Shut Down IPV6 DDOS Vulnerability. *Threatpost.*

[34] Dan Ilett of ZDNet UK reported from London, Juniper Routers Exposed to Attack, CNET.

[35] Julie Bort (2011). Microsoft, Juniper urged to patch dangerous IPv6 DoS hole.

Computerworld.

[36] Tom Mendelsohn (UK) (2016). Ipv6 router bug: Juniper spins out hotfix to thwart DDoS attacks. *ARS Technica.*

[37] Eduard Kovacs (2006). DoS Vulnerability Affects Cisco, Juniper Products. *Securityweek*.

[38] Sanjeev Kumar (2006). PING attack – How bad is it? *Computers & Security Journal, Vol. 25*.

[39] ICMP Encapsulation. last Access on DEC-09, 2016 http://home.mira.net/~marcop/even_more_tcpip.htm

[40] Kimberly Heu Department of information and Computer Sciences, Vulnerability Exploits and Countermeasures: The Ping of Death, *University of Hawaii at Mānoa.*

[41] Rodolfo Baez Jr. (2015). Evaluation of Security Vulnerabilities of Popular Computer And Server Operating Systems Under Cyber Attacks. *The University of Texas Pan American*.

[42] Mirkovic, J., Dietrich, S. Dittrich, D. and Reiher, P. (2005). Understanding a Denial of Service Attack. *InformIT*.

[43] Bipin in Security (2012). Types of Router Attacks, *Must Be Geek*.

[44] Statistics about the DDoS Attacks. ShadowServer; last Access on DEC-09, 2016. https://www.shadowserver.org/wiki/pmwiki.php/Stats/DDoSHistorical

[45] S. Kumar and R. Gade (2011). "Experimental Evaluation of Juniper Network's Netscreen-5GT Security Device against Layer4 Flood Attacks," *Journal of Information Security, Vol. 2 No. 1*, pp. 50-58. doi: 10.4236/jis.2011.21005.

[46] Del Smith CCNA (2002). “Understand the evolution of Firewalls” *Tech Republican*.

[47] Ping (networking utility). last Access on DEC-09, 2016 http://en.wikipedia.org/wiki/Ping

[48] S. Kumar and S. Surisetty (2012), "Microsoft vs. Apple: Resilience against Distributed Denial-of-Service Attacks," *in IEEE Security & Privacy*, vol. 10, no. 2, pp. 60-64. doi:10.1109/MSP.2011.147

[49] R. S. R. Gade, H. Vellalacheruvu and S. Kumar (2010). "Performance of Windows XP, Windows Vista and Apple's Leopard Computers under a Denial of Service Attack," *2010 Fourth International Conference on Digital Society*, St. Maarten, pp. 188-191.doi: 10.1109/ICDS.2010.39

[50] S. Surisetty and S. Kumar(2010). "Is McAfee SecurityCenter/Firewall Software Providing

Complete Security for Your Computer?," *2010 Fourth International Conference on Digital Society*, St. Maarten, pp. 178-181.doi: 10.1109/ICDS.2010.38

[51] Picture for ICMP Header. last Access on DEC-09, 2016
http://pixgood.com/icmp-header.html

[52] The TCP/IP Guide. last Access on DEC-09, 2016
http://www.tcpipguide.com/free/t_TCPIPInternetArchitectureandProtocolSuite.html

[53] TCP/IP Reference Page. last Access on DEC-09, 2016
http://www.protocols.com/pbook/tcpip1.html

[54] TCP Three Way hand shake. last Access on DEC-09, 2016. available online at
http://www.cisco.com/web/about/ac123/ac147/archved_issues/ipj_9-4/syn_flooding_attacks.html)

[55] S. Kumar and E. Petana (2008). "Mitigation of TCP-SYN Attacks with Microsoft's Windows XP Service Pack2 (SP2) Software," *Seventh International Conference on Networking (icn 2008)*, Cancun, pp. 238-242. doi: 10.1109/ICN.2008.77

[56] Picture for Three Way Handshake. last Access on DEC-09, 2016
http://www.networkuptime.com/nmap/images/tcp_handshake.gif

[57] Source for Firewall SYN-Proxy Image. last Access on DEC-09, 2016
https://techlib.barracuda.com/attachments/image/6979965/Generic-TCP-Proxy.PNG

[58] Security Configuration Guide for J-series Services Routers and SRX-series Services Gateways PDF. last Access on DEC-09, 2016. available online at
http://www.juniper.net/techpubs/software/junos-es/junos-es92/junos-es-swconfig-security/junos-es-swconfig-security.pdf

[59] JUNOS® Software J Series Services Routers Hardware Guide. last Access on DEC-09, 2016. available online at
http://www.juniper.net/techpubs/hardware/junos-jseries/junos-jseries96/junos-jseries-hardware-guide/j-series-hardware-guide.pdf

[60] Junos® OS Ethernet Interfaces Configuration Guide. last Access on DEC-09, 2016, available online at
http://www.juniper.net/techpubs/en_US/junos12.3/inf mation-products/topic-collections/config-guide-network-interfaces/book-config-guide-network-interfaces-ethernet.pdf

[61] J-series Services Router Quick Start. last Access on DEC-09, 2016, available online at
http://www.juniper.net/techpubs/software/jseries/junos85/jseries85-quick-start/publications-list.html

[62] Juniper router guide. last Access on DEC-09, 2016, available online http://www.juniper.net/techpubs/software/junos-security/junos-security10.0/junos-security-admin-guide/junos-security-admin-guide-TOC.html

[63] Juniper Networks, J4350 and J6350 Hardware Installation and Configuration-WBT. last Access on DEC-09, 2016. https://learningportal.juniper.net/juniper/user_activity_info.aspx?id=3379

[64] Juniper Networks, Juniper J-Series Srvices Routers: J2320, J2350, J4350, J6350 Security Policy. last Access on DEC-09, 2016. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1421.pdf

[65] Juniper J-series Services Router J4350 Getting Started Manual. *Manualslib*, last Access on DEC-09, 2016. https://www.manualslib.com/manual/80547/Juniper-J-Series-Services-Router-J4350.html

[66] DOS Attack Prevention on a Juniper M/T-Series Router. last Access on DEC-09, 2016. https://kb.juniper.net/library/CUSTOMERSERVICE/technotes/DOS_prevention.pdf

[67] Juniper Networks, Distributed Denial-of-Service Protection Feature Guide, *Juniper Networks Inc*. last Access on DEC-09, 2016. https://www.scribd.com/document/249235602/Ddos-Protection-on-Juniper-MX-Routers

[68] Picture for TCP Header Flags. last Access on DEC-09, 2016. http://www.juniper.net/techpubs/images/TCP_header_no_flags.gif

[69] Juniper J4350 Product overview. last Access on DEC-09, 2016. http://www.buyjuniper.net/Portals/1/Product%20Documents/J%20Series%20Services%20Routers%20J2320%20J2350%20J4350%20J6350%20Datasheet.pdf

[70] Wikipedia Juniper J-Series. last Access on DEC-09, 2016. https://en.wikipedia.org/wiki/Juniper_J-Series

[71] Pejahan Peymani, Matt Kolon, JUNOS Router Security, Best Common Practices for Hardening the Infrastructure. last Access on DEC-09, 2016. http://www.poplar.ru/dwnload/pdf/JUNOS_router_security.pdf

[72] Ivan Pepelnjak, Packet- and Flow-Based Forwarding, IP Space. Posted 11/30/2015.

[73] Understanding Packet-Based and Flow-Based Forwarding, *Juniper Networks*. last Access on DEC-09, 2016 http://www.juniper.net/techpubs/software/junos-security/junos-security10.4/junos-security-admin-guide/index.html?packet-flow-based-fwd-section.html

[74] Microsoft Office 365 with Excel 2013. last Access on DEC-09, 2016. https://products.office.com/en-us/microsoft-office-2013

[75] iMac Pro Server User Guide

[76] Installing IIS 8 on Windows Server 2012. last Access on DEC-09, 2016. http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012

[77] WebView Switches User Guide. last Access on DEC-09, 2016. http://www.cisco.com/c/dam/en/us/td/docs/switches/lan/csbms/srw2048/administration/guide/SR W-US_v10_UG_A-Web.pdf

BIOGRAPHICAL SKETCH

David Lee Leal was born on November 20, 1986. He finished his undergraduate studies at The University of Texas Pan American on May 2011 and earned his BS in Electrical Engineering. He has also earned his MS in Electrical Engineering from the University of Texas Rio Grande Valley in December 2016. His permanent mailing address is,

2904 North Mon Mack Road

Edinburg, Texas 78541

His Publications and Poster Presentations achieved during his Masters are:

- David Leal and S. Kumar "Can routers provide sufficient protection against security attacks?" Under review, *Journal of Information Security*