

DENIAL OF SERVICE MITIGATION USING NAT LOAD BALANCING

BY

LEE ZHI JIANG

A REPORT

SUBMITTED TO

UNIVERSITI TUNKU ABDUL RAHMAN

in partial fulfillment of the requirements

for the degree of

BACHELOR OF COMPUTER SCIENCE (HONS)

Faculty of Information and Communication Technology
(Perak Campus)

JANUARY 2017

REPORT STATUS DECLARATION FORM

Title: DENIAL OF SERVICE MITIGATION USING
NAT LOAD BALANCING

Academic Session: JAN 2017

I LEE ZHI JIANG
(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,

(Author's signature)

(Supervisor's signature)

Address:

8 JALAN USJ 6/6D

47610 SUBANG JAYA

Supervisor's name

Date: 6th April 2017

Date: _____

DECLARATION OF ORIGINALITY

I declare that this report entitled “DENIAL OF SERVICE ATTACK MITIGATION USING NAT LOAD BALACING” is my own work except as cited in the references.

The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : _____

ACKNOWLEDGEMENT

First and foremost, I will like to thank my supervisor, DR GAN MING LEE for giving me the opportunity to venture into my field of interest for this project. He proposed this network deployment as my FYP project which requires me to have hands on with real networking equipment which I have the passion of doing so. This FYP project allows me to have an idea on what I might be doing in my future career field which is network engineer.

DR GAN is an open-minded supervisor whom is experienced in the field of networking. I would like to thank him for his professional advices given to me throughout my discussion session with him. He is also willing to listen to my point of view and suggestions for this project and gave advices on further improvement.

The nature of this project requires setting up of more than two PCs, routers and switches. I also need to thank the lab assistant in FYP lab for helping me to take good care of those equipment which I left it in the lab. He also assisted me in organizing PCs setup and installing additional network cards in the PCs.

I also like to express my greatest gratitude to my friends and family that give me unconditional love, support and continuous encouragement throughout my studies in UTAR. I would like to thank my friends for their help accompanying me in lab waiting for me to finish my set up and testing process to fetch me home.

ABSTRACT

Denial of Service (DOS) or Distributed Denial of Service (DDoS) is one of the common attack that will face by any organization or anyone with various of reasons. This attack results in huge losses. Deploying anti-DDoS attack devices or equipment can be very costly and requires a lot of man power which not every organization have the resources to do so. Traditional network solution is not able to mitigate DDoS attack anymore. SDN is one of the latest technologies but it is still new so time is needed to learn it. Load Balancing is one of the method to mitigate DDoS or DOS attack by dynamically distribute the load but load balancing devices are expensive too. It also requires more time to setup and maintenance can be difficult. Most of the time, deploying expensive Load Balancing devices, IDS or IPS are redundant because they are too costly and does not perform as expected. NAT Load Balancing is also known as TCP Load Distribution. It is able to mitigate the attack by allowing the service to stay online for a longer period. Routers with NAT Load Balancing configurations are able to distribute the load to all the servers using round-robin method. Hence with the combinations of multiple servers, more resources are able to be allocated to serve the incoming huge requests. It is also a very cost effective solution with easier administration and management compared to other methods in the market. NAT Load Balancing can also be further enhanced by adding more routers and switches to create more routes to act as fail-over backup. Furthermore, by changing software configuration settings to spawn more threads to serve more requests can further enhance the efficiency of NAT Load Balancing. This method of mitigation technique is proven to be the fastest and easiest in setup and administration but also cost efficient in terms of the usage of resources especially manpower and money.

TABLE OF CONTENTS

DECLARATION OF ORIGINALITY ii

ACKNOWLEDGEMENT..... iii

ABSTRACT iv

TABLE OF CONTENTS..... v

List of Tables..... viii

List of Figures ix

List of Symbols x

List of Abbreviations xi

CHAPTER 1 Introduction 1

 1.0 About Denial of Service Attack..... 1

 1.1 Problems related to DDOS 2

 1.1.2 Organization Preparation and Readiness Against DDOS Attacks 3

 1.1.1 Business Impact on DDOS (Tim Matthews, n.d)..... 3

 1.1.3 Traditional Network Security Solutions Cannot Mitigate DDOS
 (Radware, 2013)..... 3

 1.1.4 Deploying anti DDOS device can be costly and difficult..... 4

 1.0.2 DDOS Attack Reasons (ARBOR NETWORKS, 2013):..... 4

 1.2 Importance of the DDOS mitigation OR prevention 5

 1.3 Choosing the Right Technique..... 6

 1.4 Proposed Approach 6

 1.5 Project Objectives 7

 1.6 Project Achievement 8

 1.6.1 NAT Load Balancing is implemented on the all the routers in the network.
 8

 1.6.2. Additional routers and switches are setup to create redundancy..... 8

1.6.3. The configuration file in WAMP is configured to spawn more threads to serve more requests.....	8
1.6.4. The entire setup able to mitigate a larger Denial of Service attack and larger incoming requests at the same time.	9
1.7 Background Information	10
CHAPTER 2 LITERATURE REVIEW.....	12
2.0 About Denial of Service Mitigation and Prevention.....	12
2.1 Firewall, IPS, IDS (IPS and IDS, 2011; Kening, 2013).....	12
2.2 Mitigation using SDN (Nayana et al. 2015).....	14
2.3 Cloud Services (Radware, 2013).....	15
2.4 Other General Techniques (Gupta, 2010).....	16
2.5 Comparison Of Proposed Methods With Current Available Methods.....	17
CHAPTER 3 NETWORK DESIGN AND CONFIGURATIONS.....	20
3.0 Technologies and methods used	20
3.1 Overall Network Design.....	22
3.2 Devices Configurations	24
3.2.0 Configuration Steps.....	24
3.2.1 Configuration in Routers	26
3.2.2 Configurations in Servers	28
3.3 Diagrams for Different Cases	33
3.4 Flowchart.....	36

CHAPTER 4 METHODOLOGY AND COST	37
4.1 Methodology and Approach Introduction	37
Phases of PPDIOO	37
4.2 Cost Explanation.....	39
4.2.1 Pricing of Equipment and Devices.....	39
4.2.2 Pricing of the Equipment or Devices Needed.....	40
CHAPTER 5 TESTING AND RESULTS OBTAINED	41
5.1 Testing Environment and Tools	41
5.1.1 Attack Tools	41
5.1.2 Testing Environment.....	42
5.2 Test Plan	43
5.3 Expected Results.....	46
5.4 Result Discussions and Problem Solving.....	48
CHAPTER 6 CONCLUSION	52
6.1 Project Review and Summary	52
6.2 Future Works and Improvements.....	53
Works Cited	54
APPENDIX A Running Config of Router 1.....	A-1
APPENDIX B Running config of Router 2.....	B-1
APPENDIX C BIWEEKLY REPORTS.....	C-1
POSTER.....	C- 7 -
TURNITIN PLAGARISM CHECK RESULT	C- 8 -

List of Tables

Table 2-1 Summarized Comparison of major approaches with the proposed approach
..... 18

Table 3-1 The default value of each directive of the worker MPM..... 30

Table 3-2 Explanation of each directive obtained from Apache documentation . 31

Table 3-3 Maximum values of the configuration of each directive..... 32

Table 4-1 Brief description of each of the phases in PPDIOO..... 38

Table 4-2 Pricing of the Equipment and Devices 39

Table 4-3 Pricing of the Devices Used..... 40

Table 5-1 Descriptions of Tests 45

Table 5-2 Overall Results Tabulation..... 48

List of Figures

Figure 1-1 Sample tools used to perform DDOS Attack (Gates, 2013)	5
Figure 3-2 Basic Network Setup	23
Figure 3-3 Minicom GUI Configuration Menu.....	25
Figure 3-4 Cisco CLI Configuration of Router 1	26
Figure 3-5 NAT Load Balancing Configurations CLI Commands for Router 1..	26
Figure 3-6 IP Setup Step 1	28
Figure 3-7 IP Setup Step	29
Figure 3-8 IP Address to be used.....	29
Figure 3-9 MPM Worker Module Configuration	32
Figure 3-10 Event Module Configuration.....	32
Figure 3-11	33
Figure 3-12	34
Figure 3-13	35
Figure 3-14 Request Flow Flowchart	36
Figure 4-1 Phases of PPIDOO.....	37
Figure 5-1 Command used to launch attack with time interval of 1 seconds with 100 sockets	41
Figure 5-2 HTTP Header that Solaris send to the server	42
Figure 5-3 Interface of Slowloris.....	42
Figure 5-4 Snapshot of the website hosted	43
Figure 5-5 Error message regarding insufficient threads to serve requests	49
Figure 5-6 WinNT MPM Configuration Section.....	49
Figure 5-7 Error Message when legitimate trying to access site under DOS Attack	50
Figure 5-8 Legitimate User Should Able to see this page if the website able to load	51

List of Symbols

No table of figures entries found.

List of Abbreviations

1. DOS: Denial of Service
2. DDOS: Distributed Denial of Service
3. TCP: Transmission Control Protocol
4. NAT: Network Address Translation
5. AET: Advance Evasion Technique
6. IDS: Intrusion Detection System
7. IPS: Intrusion Protection System
8. SDN: Software Defined Network
9. ISP: Internet Service Provider
10. MAC: Media Access Control
11. VLAN: Virtual Local Area Network
12. MSSP: Managed Security Service Provider
13. IP: Internet Protocol
14. NIC: Network Interface Card
15. POD: Ping of Death
16. PC: Personal Computer
17. WAN: Wide Area Network
18. SPOF: Single point of Failure
19. DHCP: Dynamic Host Configuration Protocol
20. HTTP: Hypertext Transfer Protocol
21. PCI: Periperal Compoment Interconnect
22. VAT: Value Added Tax
23. GST: Goods and Service Tax

CHAPTER 1 Introduction

1.0 About Denial of Service Attack

Distributed Denial of Service or (DDoS) or just Denial of Service attack is one of the attack that will face regularly by any organizations throughout the globe. The decrease in the cost of technologies opened a path for criminal organization or any other person with intention to initiate attacks on organization with the purpose of destruction at the minimum cost (Mikovic et al., 2005).

. There are many ways to carry out DDoS attacks but these are the three broad categories published by Arbor Networks. (Arbor Networks, 2013). These attack methods able to target Network, Session or Application Layers.

- A. Volumetric Attacks: This attack is an attempt to use up all the bandwidth of the victim network and cause network congestion to prevent another legitimate user from accessing. It also includes consuming server resources such as processing, memory and buffer resources (Palo Alto Networks Inc, 2014).
- B. TCP State-Exhaustion Attacks: An attempt to cause the connection state tables to be used up. The connection state tables are existed in a lot of infrastructure components such as load balancers, firewalls and application servers themselves.
- C. Application Layer Attacks: The target is some aspect of an application or service at Layer-7 and can be considered as the deadliest kind of attacks because it is very affective although there are as few as one machine

generating a low traffic rate.

Besides categorizing DDOS attack into these three categorizes, DDOS can also be identify as symmetric or asymmetric depending on the load of the attack traffic generated and how it spreads.

In symmetric attack, the attacker needs to use more resources to perform the attack. Usually botnets are involved in this attack. However, it is a different story for asymmetric attack, the attacker just need to make use of some internet protocol to send a relatively small amount of data but able to trigger a large reply from the victim side which resulted in huge consumption of critical resources which will cause failure.

This paper organized as follows. The first chapter contains brief explanation about Denial of Service. The explanation includes types, causes, impact and challenges faced by organization in handling DOS attack. Next, is on my proposed approach in mitigating the attack with the objectives and achievements. Chapter 2 is about reviews on the current available ways and methods to handle Denial of Service attack. The next few chapters is about the explanations about the network deployment and configurations, methodology, testing plans and methods and results. The last chapter concludes this paper by making a general conclusion which contains about the author personal insight and experience on the process of producing this paper.

1.1 Problems related to DDOS

According to RSA Conference Asia Pacific 2013, DDOS solutions provided by service provider is not adequate for 80% of the attacks that will have the most damage and there's no pre-attack reconnaissance and AET protection. (Gates,

2013). For some low profile organization or a normal person hosting web servers in their home, it is unlikely for them to face Distributed Denial of Service everyday therefore it is redundant for them to invest expensive equipment for those attack.

1.1.2 Organization Preparation and Readiness Against DDOS Attacks

Survey report by Tim Matthews also reported that there is a lack of a workable plan by organization to face and to counter targeted DDOS attacks. The number of personnel involved in incursion mitigation is high. Ideally, an organization should be able to respond with the minimum number of employees which is low as one or none.

Organizations are still relying on web applications firewalls or traditional network firewalls. It is very annoying for network administrator because distinguishing traffic sent by bots and traffic sent by a real person such as customer of an organization (Davis, 2010).

1.1.1 Business Impact on DDOS (Tim Matthews, n.d)

According to survey done by Tim Matthews from Incapsula, an Imperva company, 49% of DDOS attacks last between 6 to 24 hours with an estimated cost of 40 thousand dollars per hour. There is a large impact on units such as security, risk management, customer service and sales. There's also loss of consumer trust, customer data theft and intellectual property lost. The survey also reported that damage recovery takes months or years.

1.1.3 Traditional Network Security Solutions Cannot Mitigate DDOS (Radware, 2013)

Organizations that had firewall and IPS devices installed still became target for DDOS attack and they went offline. IPS devices can prevent intrusion

whereas firewall serve as policy enforcer by determining outgoing and incoming traffic according to rules set beforehand.

1.1.4 Deploying anti DDOS device can be costly and difficult

Startup companies or non-profit organizations might host their services with just as simple as s witch, routers and servers. There is no IPS devices installed. The organization might think it is unnecessary to invest in IDS or IPS devices because those servers or services are for their own internal usage which allowed them to access from outside the network.

1.0.2 DDOS Attack Reasons (ARBOR NETWORKS, 2013):

1. Besides the decrease in the cost of technologies, there are still several factors that contributed to the increase in DDOS attacks. ARBOR Networks also discussed a few in one of their publication is 2013. “It is not just financial institutions and gaming sites which are being targeted, we have seen government departments hit, e-commerce sites and even pizza delivery companies being targeted. Why this change? Well, there are a number of reasons” (ARBOR NETWORKS, 2013):

Two out of three reasons are chosen to highlight here:

1. Attack tools are easily to be downloaded online: The tools available online can be downloaded and used by anyone therefore any person or organization or even state that is looking for a way to impact other internet users can have access to these tools easily. RSA Conference Asia Pacific 2013 also highlighted that any device with an IP Address can be used to launch an attack. Examples of attack tools also presented in the conference such as

HOIC, Hping3, LOIC, Dirt Jumper and etc. Figure 1-1 shows the demonstration of attacks using those tools. (Gates, 2013)

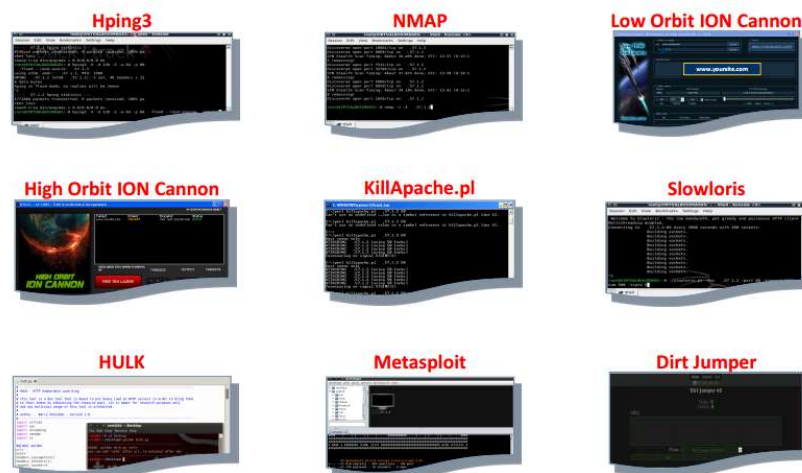


Figure 1-1 Sample tools used to perform DDOS Attack (Gates, 2013)

2. It is easy to hire botnets to do DDOS: There may be a temporally economic decline but the botnet economy continues to grow well. Hiring botnets to carry out DDOS campaign on your behalf is easy. Many sites are offering this at a reasonable and competitive rate.

1.2 Importance of the DDOS mitigation OR prevention

DDOS prevention can act as first layer of defense, but if the first layer of defense is broken, DDOS attack must be mitigate to minimize the impact. The issue is about the availability of the services when there's a DDOS attack. The availability need to be ensure legitimate user still able to access the services. This is to minimize the impact on daily operation of an organization even there's a DDOS attack.

1.3 Choosing the Right Technique

Denial of Service or Distributed Denial of Service is a common problem faced by many organizations. In most of the times, organization will face a huge number of requests during a certain period. Many servers or services has a particular limit on how many requests they can serve at the certain period. Requests that made after the server exceeds the limit will not be served. This situation is similar with Volumetric Denial of Service Attack.

It is costly and redundant to deploy anti DDOS device because there are many other attacks beside DDOS that an attacker could use to take down a particular service. Certain devices only perform specific function such as Load Balancer only balance the load by routing packets according to predefined algorithm. Firewalls only prevents attack according to pre-defined rules. It is a waste of resources to purchase or implement equipment that are not able to counter new type of attacks.

Besides that, huge number of requests doesn't happen daily for most of the organization. Higher number of requests are only expected during holiday seasons or promotion is made that is enough to attract huge number of people. Therefore, it is not wise for an organization to upgrade or bought new equipment just because they faced huge number of requests during a certain period.

1.4 Proposed Approach

The proposed approach in tackling this issue is by using NAT Load Balancing and multithreading on the servers. This can be further enhanced by adding redundancy. Redundancy can be introduced by utilizing Dual WAN connection of an organization. In redundancy, there are additional routers and switches to create more routes. These additional routes will be act as fail over and able to be used when the original route is not functioning. Besides failover, it also can be used as Load Balancing to reduce the traffic on the particular route.

This approach is not just cost efficient but also environmental friendly as the need of purchasing new equipment is optional yet able to achieve optimum results in most of the situation. Optimum result refers to moderate scale of Denial of Service Attack able to be mitigated and increased requests will have minimum impact on the entire system. In simple words, a legitimate user will be able to be served even when there is a Denial of Service attack or the current traffic is larger than usual.

Cost refers to money, time and man power. This approach can be implemented on the spot in less than 3 hours by just only one person with the condition that the person in charge has intermediate skills in the particular products and computer literate in terms of making advance configurations. No programming is needed but knowledge on Operating System is necessary. This is the basic requirements for every IT personnel in an organization and this skill can be picked up easily by non-IT background person as long as he or she is computer literate.

This project requires current devices which includes network equipment devices such as servers, switches and routers to be reconfigured as a new revamped network setup. Previous configurations will be cleared. New software or firmware have to be installed on servers and network equipment respectively if necessary as the project progress. Configurations done on the server requires administrative privileges.

1.5 Project Objectives

1. To simulate and understand the impact of DOS and DDOS attack using TCP State Exhaustion and Volumetric Attack.
2. To implement NAT Load Balancing at the router.
3. To prove that NAT Load balancing able to mitigate Volumetric or TCP State-Exhaustion Attack or both.
4. To simulate the attack with NAT Load Balancing enabled and understand, observed the maximum extend of the load balancing can do to mitigate the attack.
5. To prevent Single point of failures by adding more routers and create more routes.
6. Improve the mitigation by using spawning more threads.

This project does not cover designing a new algorithm for load balancing. Only existing feature in the router will be used. This project does not focus on preventing, blocking or recovering from the attack. In the case that the attack last for a very long time, it is not guarantee the period the service will stay online. It is still depending on the capacity of the particular device or server. Last but not least NAT Load Balancing able to mitigate Volumetric attacks and TCP-State exhaustion attack only with the assumption that the router has much more state tables than the servers. The amount of attack mitigated is very much depending on the configurations and resource allocation of the servers that are used for load balancing purpose.

1.6 Project Achievement

1.6.1 NAT Load Balancing is implemented on the all the routers in the network.

CLI commands to perform TCP Load Distribution are configured on the routers. TCP traffic that targeted certain port or service is distributed across the PCs across the network. The service is still accessible from outside network even though one PC is down.

1.6.2. Additional routers and switches are setup to create redundancy.

The initial configuration is only one router and one switch. Adding one extra router and switch, the network becomes more reliable. Since there are two routers, Dual Wan connection is supported for fail over mode and load balancing mode. Fail over mode is implemented in which the service is still accessible by using another IP Address even when one of the router or the switch is not working properly.

1.6.3. The configuration file in WAMP is configured to spawn more threads to serve more requests.

By default, the number of threads spawned by Apache service to serve HTTP request

is set at a minimum level to ensure other programs or processes will not be affected. However, that amount can be increased by 2 times without affecting other programs running in the PC and at the same time allow more requests to be served. The time taken to cause a Denial of service is extended.

1.6.4. The entire setup able to mitigate a larger Denial of Service attack and larger incoming requests at the same time.

With the combination of NAT Load Balancing, additional routers and switches and spawning more threads, the entire network is able to mitigate a larger scale of Denial of Service Attack and also cater more incoming requests when needed.

1.7 Background Information

Before proceeding, there are a few terms need to be explained here. Denial of Service so called DOS is an attempt by using any method to make the server down or inaccessible by others. The most common one is overload the server causing insufficient resources to handle others request.

NAT is Network Address Translation is a technique that used in a router to translate private IP Address to Public IP Address so called WAN also known as Internet. It also works vice versa by translating public address back to a particular private IP Address.

Port Number is a number assigned after an IP Address to indicate the serviced use or a particular host inside the private IP network. If it is used to indicate a particular host inside a private network, the port number can be from 1 up to 65535 and is added at the back of the WAN IP Address. The WAN IP Address can also still belong to the private IP range.

TCP is Transmission state protocol and it is one of the important protocols in the Internet. Web servers and File servers are relying on TCP. It uses the 3-way handshaking. The initiator need to send a SYN request to the server, then the server reply with SYN-ACK. At last the client send an acknowledgement back to the server then only the connection is established. This is the part where a DOS attack can be issued. An attacker can send many SYN packets but do not want to acknowledge it causing the entries in the TCP state table to use up.

Kali Linux is a type of Linux Operating System mainly use for security penetration testing. Linux is an Operating System just like Windows, but Linux is UNIX based whereas Windows is DOS based.

Dual WAN means there are two internet connections connected to the network of particular organization. It normally serves as a backup purpose in case one of the internet connections is down. In most cases, both of the internet connections are supply by different ISP.

Load Balancing in computing means the distribution or allocation of loads to more

than one resource that perform computational activities which includes computers, network links, and other end devices. The distribution of loads to all the devices is to reduce the load on a single device.

A thread is a single sequence of execution in operating system. Multiple threads can exist in a single process executing tasks concurrently. In a more simpler way multithreading can be described as a group of helpers are helping to perform the same tasks together which resulted in more activities can be completed within certain time frame. The helpers are controlled by their master which is the process.

CHAPTER 2 LITERATURE REVIEW

2.0 About Denial of Service Mitigation and Prevention

To begin with, many organizations have their own way of DDOS prevention as well as DDOS mitigation. There are many anti DDOS services available offered by service provider. Besides that, there are also a diversity and variety of equipment and devices that can be installed to prevent or mitigate DDOS attack. This section will explain and discuss about current practice and solution used by organization to defend against DDOS attack as well as solutions offered by service provider.

2.1 Firewall, IPS, IDS (IPS and IDS, 2011; Kening, 2013)

There are still many organizations stick to traditional security tools. Firewalls and Intrusion Prevention Systems are two of the examples. They believe that IPS and firewalls still able to help. (IPS and IDS, 2011)

IPS systems are deployed with the purpose of blocking the attack by adding the attacker IP address to a blocked list for a certain period of time or permanently based on certain predefined rules. IPS systems also able to detect and recognize port scans with the intention to find loop holes or available ports within an organization network to launch an attack. IPS system also has other advance features besides blocking, dropping packets and logging. They are capable of sensing and stopping possible attacks. (IPS and IDS, 2011)

An IDS system only detects intrusion, log the attack and send alerts to administrator. IDS systems do not block, drop or sense packets therefore the network performance can still maintain at optimum level. (IPS and IDS, 2011)

However, devices that integrate IDS and IPS together are available in the market.

IDS are used first to log the activities then IPS will use the logs to tune the system such as setting up defined rules. (IPS and IDS, 2011)

IDS and IPS are required because firewall is only a policy enforcer by controlling incoming and outgoing traffic according to address, ports and type of service. Certain traffic will still pass through. Firewall is not as smart as IDS to tell whether the traffic is legit and normal. (IPS and IDS, 2011)

Despite IDS and IPS have the ability to sense the attack but there are several issues for considerations. If IDS and IPS systems are not fine-tuned, false positive results will occur as legitimate traffic will be blocked. IDS will just send the alerts and log the false positive attack. Some administrators do not prefer system to take action on their behalf but they prefer to look at the alerts and decide the actions to take. (IPS and IDS, 2011)

IDS and IPS are just like any other network equipment. They need to be configured before deployment. Besides, maintenance also required. Configurations and maintenance required time and man power. Certain organization might not have the resources to do so.

In addition, IDS and IPS can be considered as extra equipment or device to be purchase by an organization if the organization intended to use it.

Actually IDS, IPS and firewalls can be considered as traditional security tools and cannot be use to handle DDOS attacks. Firewalls and IPS can only concentrate on examining and preventing the intrusion one entity at a time. They are not designed to detect the combined behavior of legitimate packets sent millions of times. (Kenig, 2013).

Firewall and IPS are devices that track all connections and store them in a connection table then every packet is matched against the connection table to verify the

legality. The problem is during DDOS attack the connection table will be used up very quickly because a new connection will be opened in the connection table for each malicious packet. Once it is used up, legitimate user will unable to establish new connection. However, DDOS mitigation devices are stateless devices in which they can handle millions of packets without exhausting the connection tables. (IPS and IDS, 2011)

2.2 Mitigation using SDN (Nayana et al. 2015)

The concept of SDN is instead of using switches to forward packets, there is a controller to make decision for traversal of packets. The controller can identify the topology by listening to the switches. The available path with minimum load can be calculated by the controller. The controller can instruct the switches to forward the packets to that path with minimum load. By doing this the load can be balanced effectively

SDN perform DDOS mitigation by letting the DDOS mitigation controller first detects the attack by using threshold value and SDN network monitoring and security are state of the art creation. Network management and complexity are able to be reduced by using SDN. It can balance the network and provide security by using programs. Besides, the SDN controller make obtaining global view of network states and centralized networking possible. Human will no longer needed to handle the management and maintenance work of DDOS mitigation schemes. Installation of specific devices is unnecessary as mitigation and load balancing functions are abstracted and integrated at the application layer of SDN.

SDN can make reconfiguration of ISP routing tables easier to counter semantic, brute force or flooding attack. This requires the cooperation of ISP and this configuration is quite complex using traditional methods. Although SDN able to make things easier but it is useless if ISP do not want to do so or they do not want to implement SDN for the reconfiguration process.

SDN guarantees dynamic network and programmable network control and it reacts faster with more efficiency. However, SDN is still new and progressing and there are IT professionals are not ready for investment in SDN yet due to several reasons. (David, n.d). They are worry about will their current IDS or IPS equipment will not function well when SDN is implemented. IDS and IPS works by tapping into range of ports or a particular port to replicate the entire traffic of a VLAN or network segment for sniffing. Traditional switch hardware and software replicate that traffic and serve it into the IDS/IPS system. In contrast, SDN uses a hypervisor and general OS routines to replicate the traffic. Tests also have proven that SDN loses approximately 25% to 30% of attack vector events.

Besides fault in SDN software will cause problems in tracking MAC addresses for devices that connected to the wired and wireless network. The MAC addresses recorded are incorrect.

The major problems related to SDN is lacking of familiarity and absence of standard skills on SDN. The dynamic infrastructure of SDN hasn't been seen yet therefore investment will not be made unless they are able to have hands on to experience it. In order for a network engineer to understand SDN, they need the skills but they do not know where to start as SDN strategies are unclear.

2.3 Cloud Services (Radware, 2013)

With the rise of DDOS attacks and lacking of space in particular organization due to high rental rate, organizations rely on cloud services to serve their clients or customers. Many ISP and MSSP had started offering anti-DDOS services. They can prevent organizations from network flood attacks by deploying equipment for mitigation at their side. This can make sure network flood attacks will be blocked before reaching the organizations.

Cloud services also offered distributed computing whereby there are mirror servers located at different places. They can be used for load balancing purpose and backup in case one of them is down due to DDOS attack. This service can be

a monthly or yearly subscription basis.

However, cloud based anti-DDOS fail to block application DDOS attack and low and slow attacks because their mitigation equipment has low sensitivity in detecting such kinds of attacks in the cloud. In addition, MSSP must host the SSL keys of the protected enterprise for SSL based attack detection. This is the problem because it is related to compliance and regulatory concerns of the protected enterprise which cannot provide its SSL keys to others including MSSP therefore enterprise data center will receive SSL based attacks without any mitigation.

When there is an attack, diversion of traffic is required form the protected enterprise into the MSSP scrubbing center. This diversion is not automatic because it requires human involvement which last for at least 15 minutes in which the online services are exposed to the attackers because they are not protected.

2.4 Other General Techniques (Gupta, 2010)

The techniques discussed by Gupta are disabling unused services, using global defense infrastructure and IP hopping.

Disabling unused services by reducing the number of open ports in hosts is to reduce the chance for an attacker to exploit the vulnerabilities. It is not very effective because the intension of DDOS is to cause a legitimate cannot use a particular service. The open ports are meant to provide the service therefore it is useless to close other ports as the attacker only interested in attacking the service they offered.

Global defense infrastructure can prevent many form of DDOS attack by applying filtering rules. However global defense architecture is possible only in theory because Internet is administered by various autonomous systems according to their own local security policies.

Changing of IP addresses or location of the active server from a pool of homogenous servers or pre-specified set of IP address ranges can prevent DDOS attacks. This action will still leave the server vulnerable because the attacker can

always launch the attack at the new IP address. Besides that, the new IP addresses are easy to figure out using Domain name resolver. Another issue about keep changing IP Address is there might not be enough public address for a particular server or host to change.

There are still many other ways of DDOS mitigation and prevention and almost all of them requires purchasing new equipment, learning new skills, editing or writing complex scripts or subscribe to other services. All of these require will incur an amount of cost, manpower and time. The issue about cost can be resolved by using existing or refurbished equipment with revamped and different configurations.

2.4 Comparison Of Proposed Methods With Current Available Methods

	Firewall	IDS	IPS	SDN	Load Balancer	Cloud Services	Disable unused services	Global Defensive Infrastructure	Proposed Method
Cost	High			Appears to be low but high hidden cost	High	Moderate	Very Low	Uncertain	Very Low
Speed Of Deployment	Slow. Requires study of documentation and manuals before perform configurations. Understanding of certain knowledge beforehand is necessary.					Fast	Fast	Uncertain	Fast
Effectiveness	Moderate			Effective	Effective	Depends	No	Uncertain	Yes
Ease of Maintainence	Difficult			Yes	Uncertain	Yes	Yes	Uncertain	Yes
Ease Of Deployment	Difficult, due to extensive planning needed and unfamiliarity.					Yes	Yes	Uncertain	Yes
Integration Friendly	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 2-1 Summarized Comparison of major approaches with the proposed approach

Table 2-1 shows the rating of all the methods explained from 2.1 to 2.4 in terms of cost, speed of deployment, effectiveness, ease of maintaining and ease of deployment.

With comparison with other methods, the proposed approach is the best solution among all other methods mentioned in the table. The current approach works similarly like a load balancer however it cannot compete with the current approach in terms of cost, ease of deployment and maintenance and speed of deployment.

CHAPTER 3 NETWORK DESIGN AND CONFIGURATIONS

3.0 Technologies and methods used

This project approach is making use of **Rotary NAT**. Rotary NAT is an improved form of port forwarding. The concept of NAT is briefly explained in section 1.7. For most organization, the type of NAT implemented are Port Address Translation and Port Forwarding for the purpose of providing internet access and to allow their customers to access their services hosted on the computers that are connected to the network. Port forwarding can be classified as the traditional form of NAT. The same port in the internal network can only be used once. For example, if the web server already taken port 80, then other devices on the network cannot host websites using port 80 anymore. This also creates the issue of port clashing in some network. New routers will have their own web console which will utilize port 80 for GUI based configuration hence the person who accesses the public IP with port 80 will be greeted with the router login menu instead of the website.

By using Rotary NAT, TCP Load distribution is made possible if there are multiple servers in the network. Load distribution can be done by all the servers that are connected to the same network by forwarding packets evenly to all the servers. In Rotary NAT, a virtual server is established in the inside network which communicates with real servers. Destination addresses that match an access-list are replaced with address from the IP address rotary pool. Round robin algorithm is used to perform the allocation. The destination address **is the IP Address used by outside network to access the particular service which will be the public IP Address** also called as WAN IP address. However, prior to Rotary NAT implementation the web server of the router need to be disabled or any other services hosted by the router.

Next **redundancy** is implemented by adding one additional router and one switch. Additional network cards are added to the servers so that it is connected to the extra switch which is also connected to extra router. The extra router is connected to the

internet using the second internet line provided by the ISP.

Multithreading is also used on the servers. More threads are spawned to serve the request. The basic functionality of threads and multithreading is explained in 1.7

Last but not least the optionally method can be implemented is Round-Robin DNS as an extension to the redundancy method in adding the extra router and introduce one extra public address. Round-Robin DNS is to resolve single domain name to multiple IP-address in a round robin manner according to the sequence set in the address pool list.

3.1 Overall Network Design

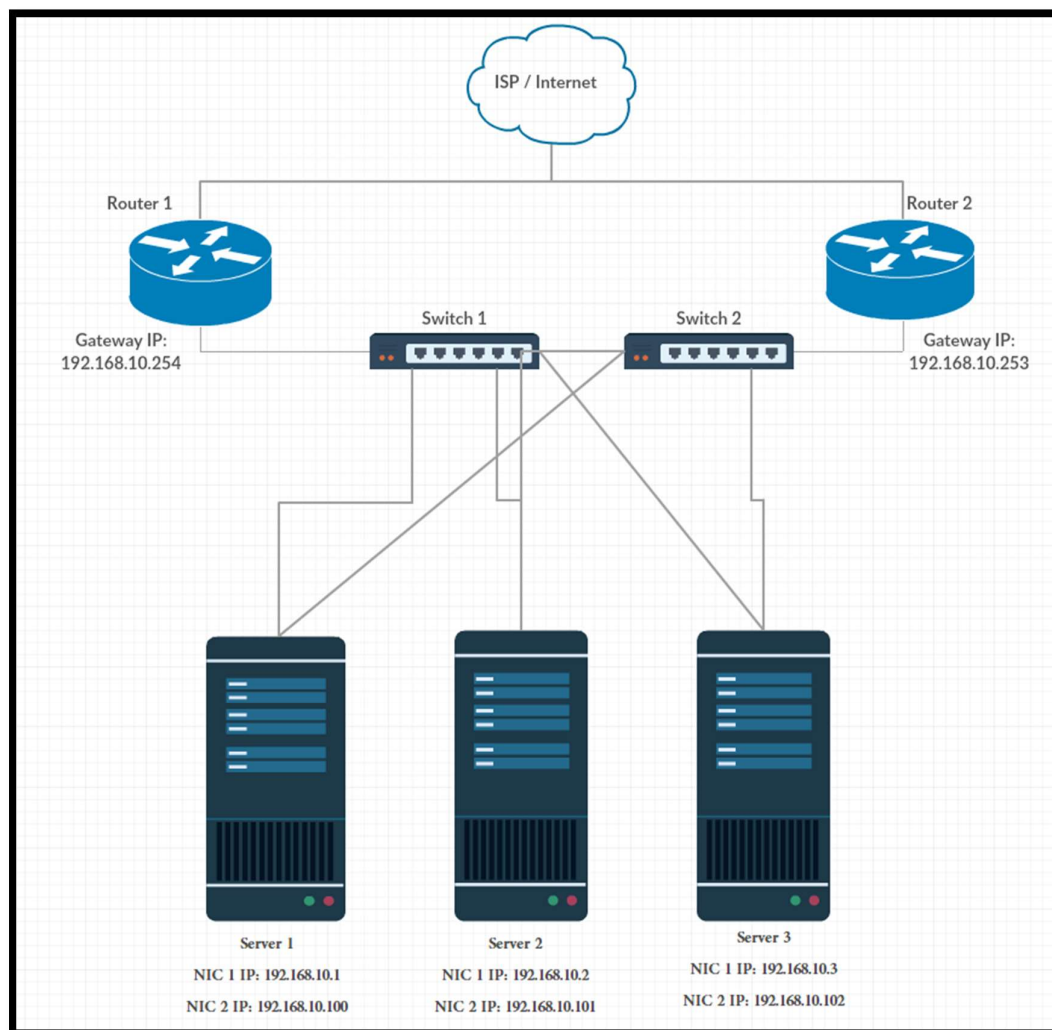


Figure 3-1 Overall Network Design

Figure 3-1 describe the overall network design for this approach. There are WAN connected two routers connected to two switches. Both of the switches are also connected to each other and each of the switches is connected to the 3 same servers which are providing web service.

Both of the routers are configured with NAT Rotary which distributes packets and requests to all the 3 servers.

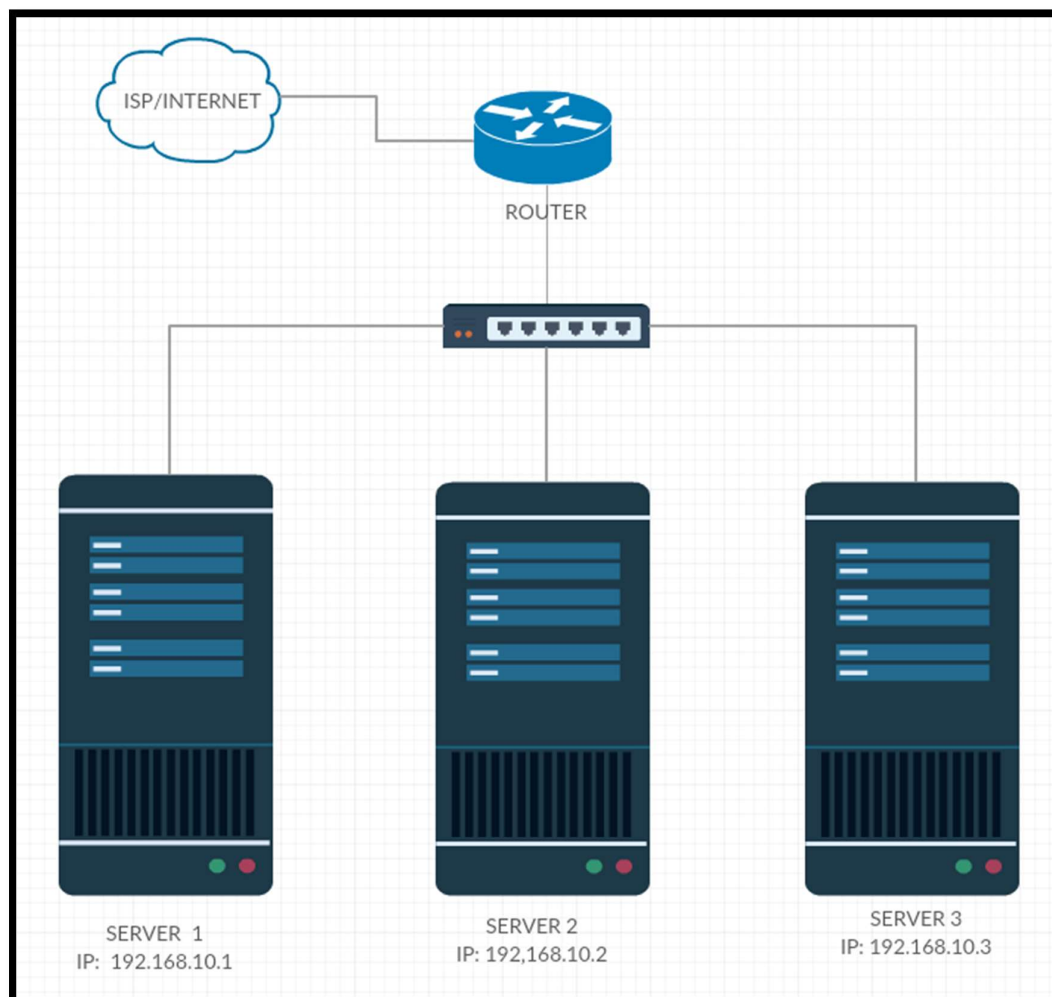


Figure 3-2 Basic Network Setup

Figure 3-2 illustrate the basic network setup. The overall network design illustrated in Figure 3-1 is the result of combination of 2 network setups in Figure 3-2. In Figure 3-1 the configurations are almost the same except for the default gateway IP Address and the IP ranges of the NAT Rotary pool list.

There is an assumption that Round Robin DNS or similar load balancing technique is configured at the ISP site or domain hosting site to forward the requests to the public IP Addresses of both routers.

3.2 Devices Configurations

3.2.0 Configuration Steps

Cisco devices configurations are done using both CLI and web GUI commands. The higher-level configurations are done using web based GUI whereas the lower level configurations (couldn't be configured from GUI menu) is configured using CLI commands.

CLI Configurations need to be done via the console port of the Cisco device. A serial cable connects the console port of the device to the serial port of the PC which is running Linux.

Minicom is one of the serial text based serial communication program that runs under Linux however configuration is necessary before use.

Minicom Installation

In Ubuntu / Debian Linux:

```
$ sudo apt-get install minicom
```

For Red Hat / Cent OS / Fedora:

```
# yum install minicom
```

Minicom Setup

```
$ minicom -s
```

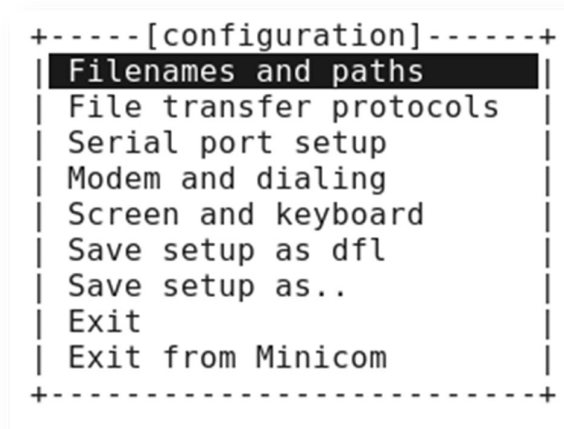


Figure 3-3 Minicom GUI Configuration Menu

Figure 3-3 shows the configuration menu of minicom. The COM port number of the serial port need to be configure in “Serial Port Setup”

Using Minicom to connect to the Cisco device

\$ minicom -c on

3.2.1 Configuration in Routers

```
interface FastEthernet0/0
description $FW_OUTSIDE$
ip address dhcp
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
service-policy output SDM-QoS-Policy-1
!
interface FastEthernet0/1
description $FW_INSIDE$
ip address 192.168.10.254 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
no mop enabled
!
```

Figure 3-4 Cisco CLI Configuration of Router 1

Interface FA 0/0 is connected to the WAN. The IP Address of the interface is obtained using DHCP. Interface FA0/1 is the private network of 192.168.10.0/24. NAT is configured such as all the devices in FA0/1 have access to the Internet using Port Address Translations Method.

For Router 2 the gateway IP Address will be: 192.168.10.253.

```
no ip http server
no ip http secure-server
ip nat pool ROTATE 192.168.10.1 192.168.10.3 prefix-length 24 type rotary
ip nat inside source list 11 interface FastEthernet0/0 overload
ip nat inside destination list LOADBALANCE pool ROTATE
!
ip access-list extended LOADBALANCE
permit tcp any host 192.168.237.60 eq www
permit tcp any host 192.168.237.61 eq www
permit tcp any host 192.168.237.62 eq www
permit tcp any host 192.168.237.63 eq www
permit tcp any host 192.168.237.64 eq www
```

Figure 3-5 NAT Load Balancing Configurations CLI Commands for Router 1

The term “rotary” is the key term for TCP load distribution. Any incoming connection that use the IP Address of INT FA0/0 will be forwarded to range from 192.168.10.1 to 192.168.10.3 in round robin basis for connection coming in using Router 1.

However, for Router 2, the packets and requests will be forwarded to the range from 192.168.10.100 to 192.168.10.103

The ACL is setup to allow the forwarding of packets of the interface IP to the IP Address set in the pool using PORT 80 ONLY. The IP Address range stated in the CLI commands are the IP range for the servers that host the website.

3.2.2 Configurations in Servers

Servers' configurations involve two parts. The first part is configuration of IP Address of NIC. The second part is configuration on the config file of Apache server to spawn more threads.

Part A: NIC IP Address Configurations

The servers' operating systems are Windows 7. IP Addresses are configured in Control Panel\Network and Internet\Network Connections. IP Address is configured by using the properties window of the network adapter.

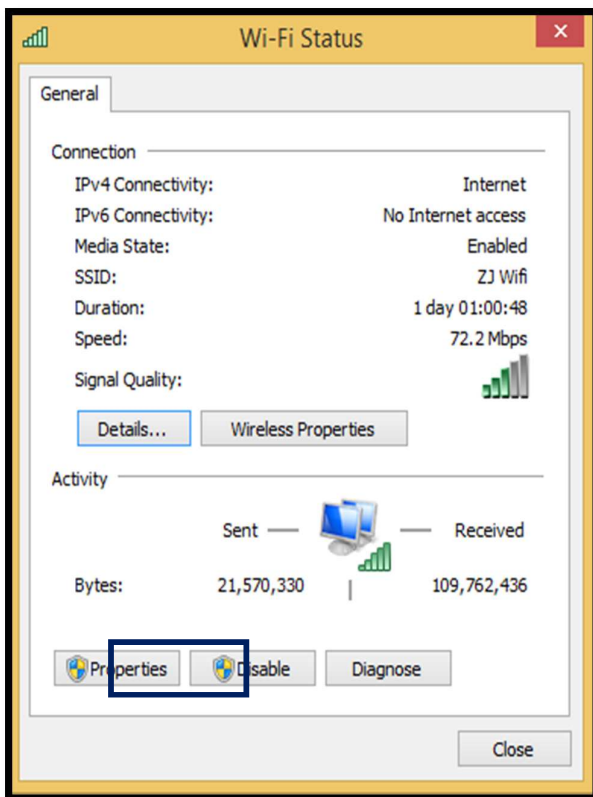


Figure 3-6 IP Setup Step 1

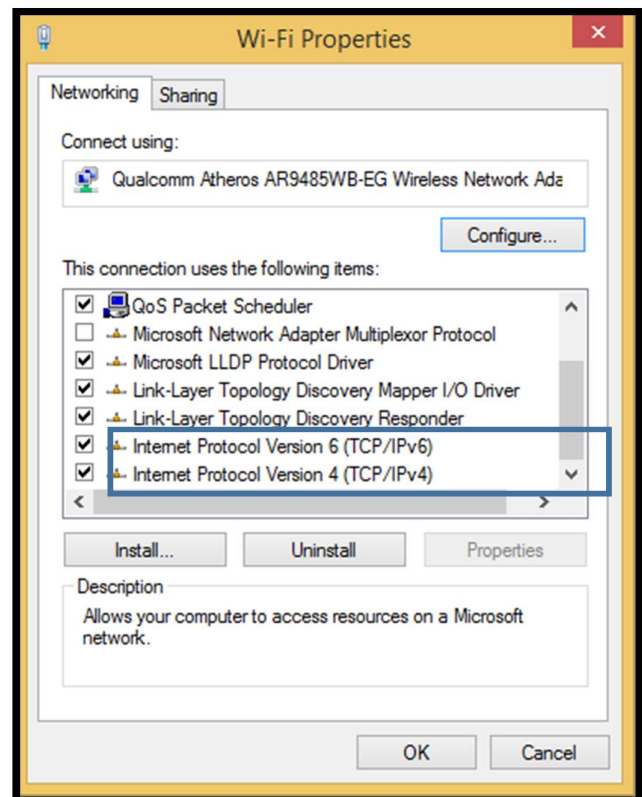


Figure 3-7 IP Setup Step 2

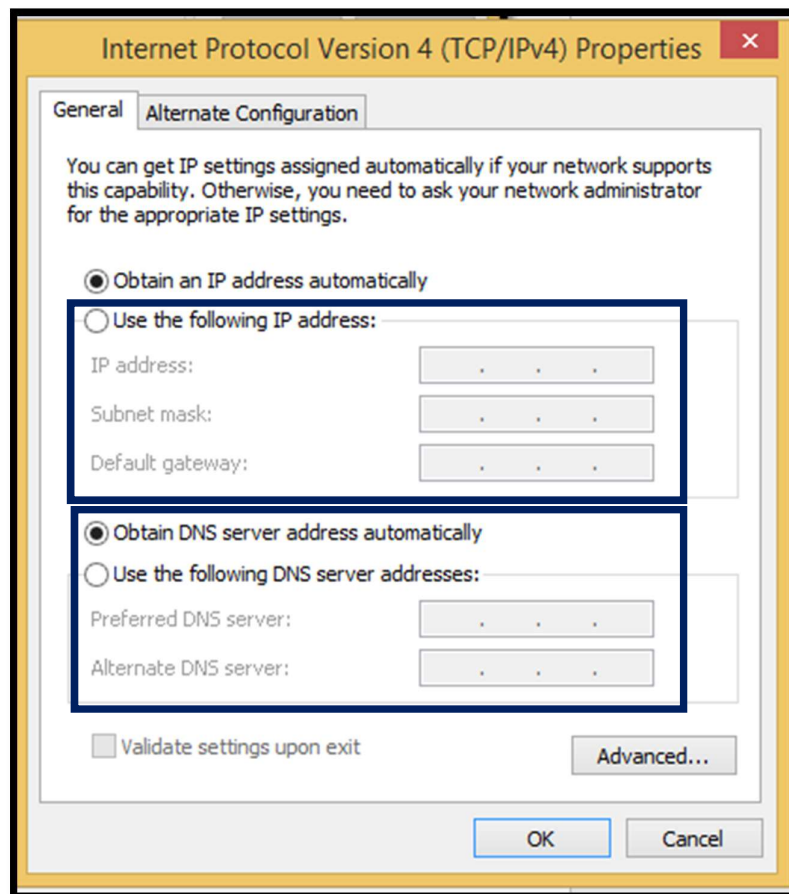


Figure 3-7 IP Setup Step 3

Figure 3-6 to Figure 3-8 illustrate how to configure static IP Address for a particular network adapter. There is a strict guideline to follow which is the IP Address and Gateway for both network adapters must be different but both of them can be under the same network. The warning message regarding about same network id can be ignored.

IP Address: 192.168.10.1 – 192.168.10.3 Subnet Mask: 255.255.255.0 Default-Gateway: 192.168.10.254
IP Address: 192.168.10.100 – 192.168.10.102 Subnet Mask: 255.255.255.0 Default-Gateway: 192.168.10.253

Figure 3-8 IP Address to be used

Part B: WAMP Configuration on Apache Service

Apache is the service or process that is responsible for serving http request. There is a config file located in the “extra” folder under the Apache directory. The file name is called “httpd-mpm.conf”. This is the config file for Server Pool Management also called as Multi Processing Module. It provides portable multiprocessing to Apache HTTP Server. There are a lot of modules in this config file, but the module used is the **worker** module.

The worker module implements a hybrid multi-threaded multi-process web server, for UNIX version of Apache HTTP Server. It is able to serve large number of requests with fewer system resources compared to a process-based server. ("MPM or Multi Processing Module - How to LAMP"). Proper configuration of this config file can drastically increase the bottlenecks of the web servers.

According to Apache documentation, child process is started by a single control process. The number of server threads created by each process is fixed as specified in the ThreadsPerChild directive. There is also a listener thread which listens for connections and passes them to a server thread for processing when they arrive.

Apache server has a pool or idle spare threads, which stand ready to serve incoming requests therefore there is no need for client to wait for new process or threads to be created. Their requests can be served almost instantly.

Table 3-1 shows the configuration of the process-thread controls in the worker MPM.

Directive	Default Value	Values in Unknown
ServerLimit	16	<i>a</i>
StartServers	2	<i>b</i>
MaxRequestWorkers	400	<i>c</i>
MinSpareThreads	25	<i>d</i>
MaxSpareThreads	75	<i>e</i>
ThreadsPerChild	25	<i>f</i>
MaxConnectionPerChild	0	<i>g</i>

Table 3-1 The default value of each directive of the worker MPM

Directive	Explanation
ServerLimit	Hard limit on the number of child processes. Condition: $a \geq \frac{c}{f}$
StartServers	The number of processes that will initially launch.
MaxRequestWorkers	The maximum number of clients that may be served simultaneously. The maximum total number of threads in all processes
MinSpareThreads	Minimum number of idle threads available to handle request spikes
MaxSpareThreads	Maximum number of idle threads
ThreadsPerChild	Number of threads created by each child process
MaxConnectionPerChild	The number of connections that an individual child server will handle during its life

Table 3-2 Explanation of each directive obtained from Apache documentation

Directive	Default Value
ServerLimit	16
StartServers	3
MaxRequestWorkers	4000
MinSpareThreads	75
MaxSpareThreads	250
ThreadsPerChild	1000
MaxConnectionPerChild	0

Table 3-1 Maximum values of the configuration of each directive

```

<IfModule mpm_worker_module>
    ServerLimit          16
    StartServers         3
    MinSpareThreads      75
    MaxSpareThreads      250
    ThreadsPerChild      1000
    MaxRequestWorkers    4000
    MaxConnectionsPerChild 0
</IfModule>

```

Figure 3-9 MPM Worker Module Configuration

```

<IfModule mpm_event_module>
    StartServers         3
    MinSpareThreads      75
    MaxSpareThreads      250
    ThreadsPerChild      1000
    MaxRequestWorkers    4000
    MaxConnectionsPerChild 0
</IfModule>

```

Figure 3-10 Event Module Configuration

Figure 3-10 and 3-11 illustrate the changes did in the file called “httpd-mpm.conf”. According to the comments written in the config file only one module need to be configured as only one section or module will be relevant to the installed httpd. However, the event module is configured also for try and error purposes. It does not revert back to the default values since it does not affect any of the configurations.

In order for http-mpm.conf to work, the config file must be included in the main config file of Apache which is httpd.conf using include */conf/extra/httpd-mpm.conf*.

3.3 Diagrams for Different Cases

Case 1: Normal Cases all network devices are running properly

1.1 User visit the website using public IP Address of Router 1

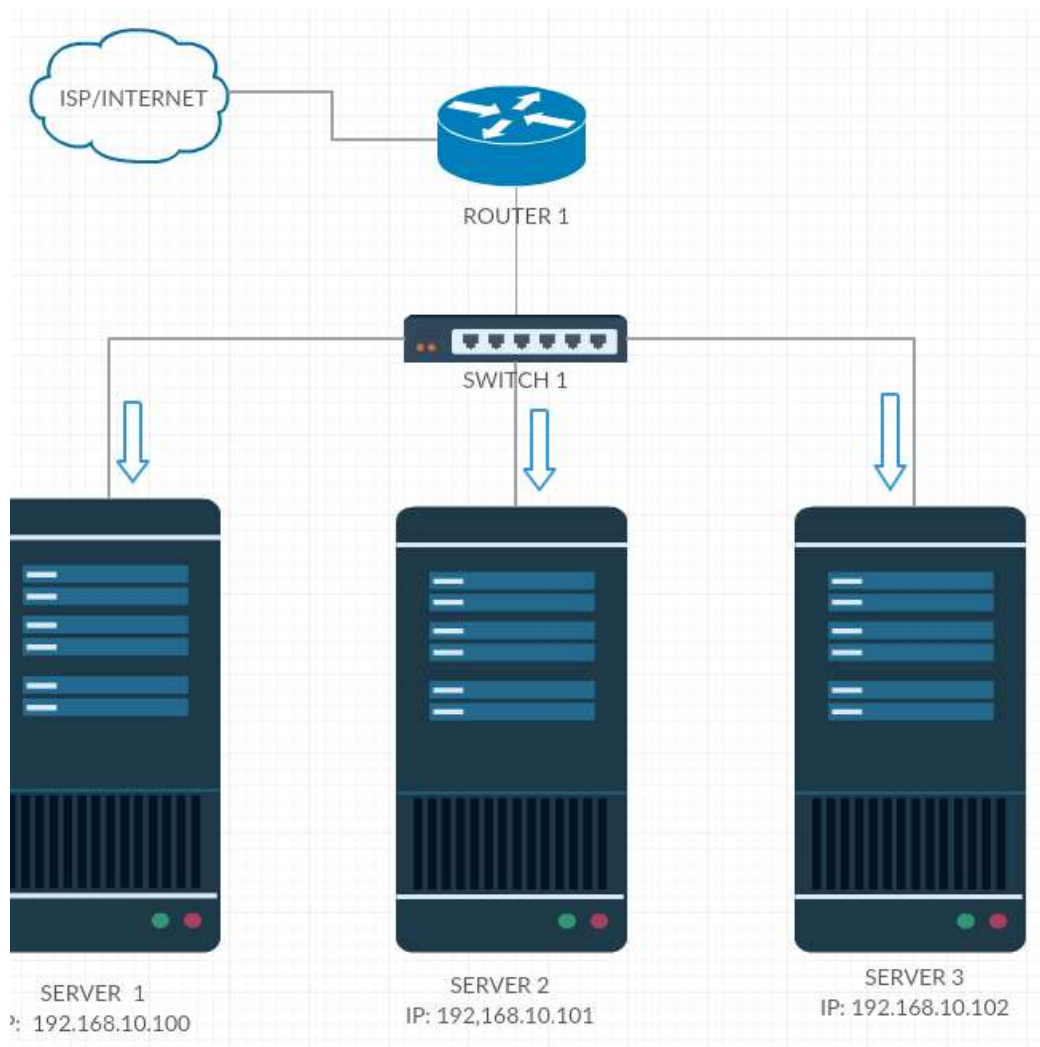


Figure 3-11

1.2 User visit the website using public IP Address of Router 2

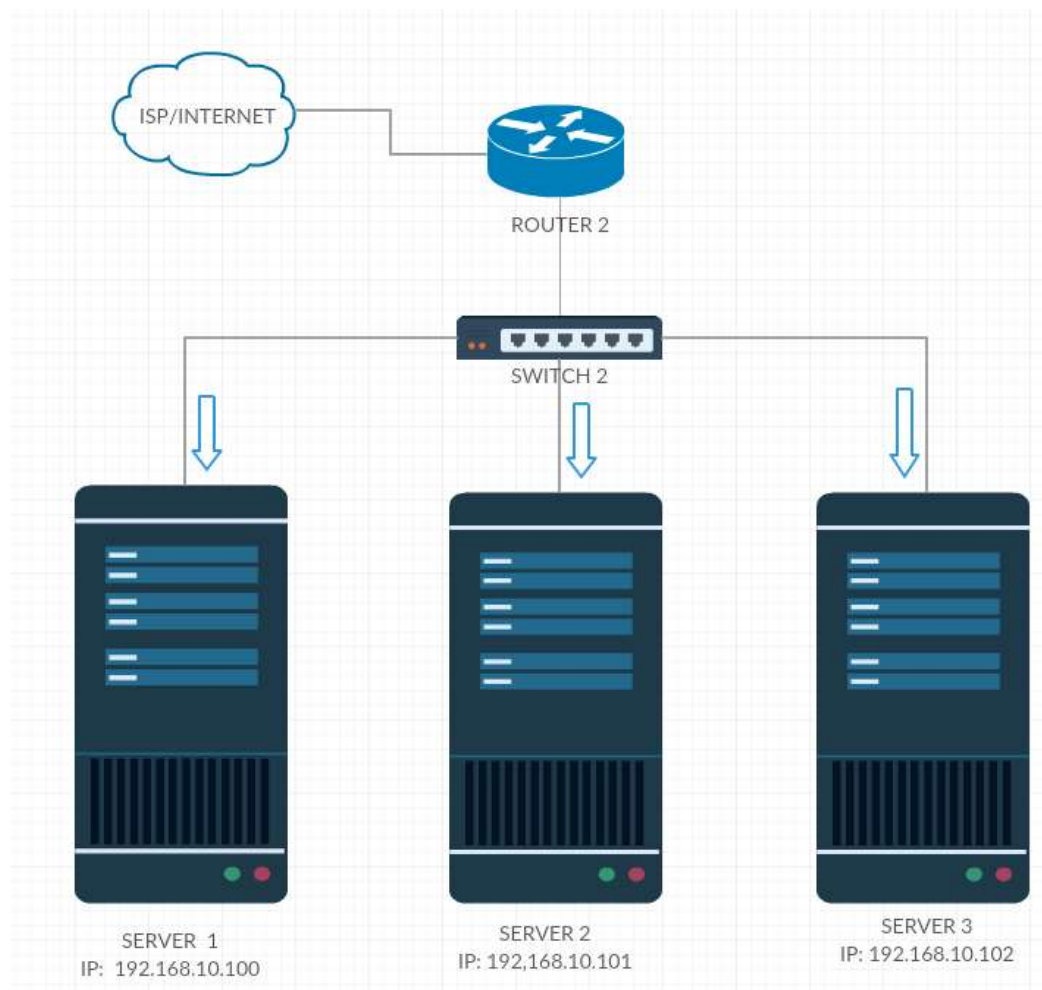


Figure 3-12

Case 2: Failure of certain equipment or devices

2.1 One server is down.

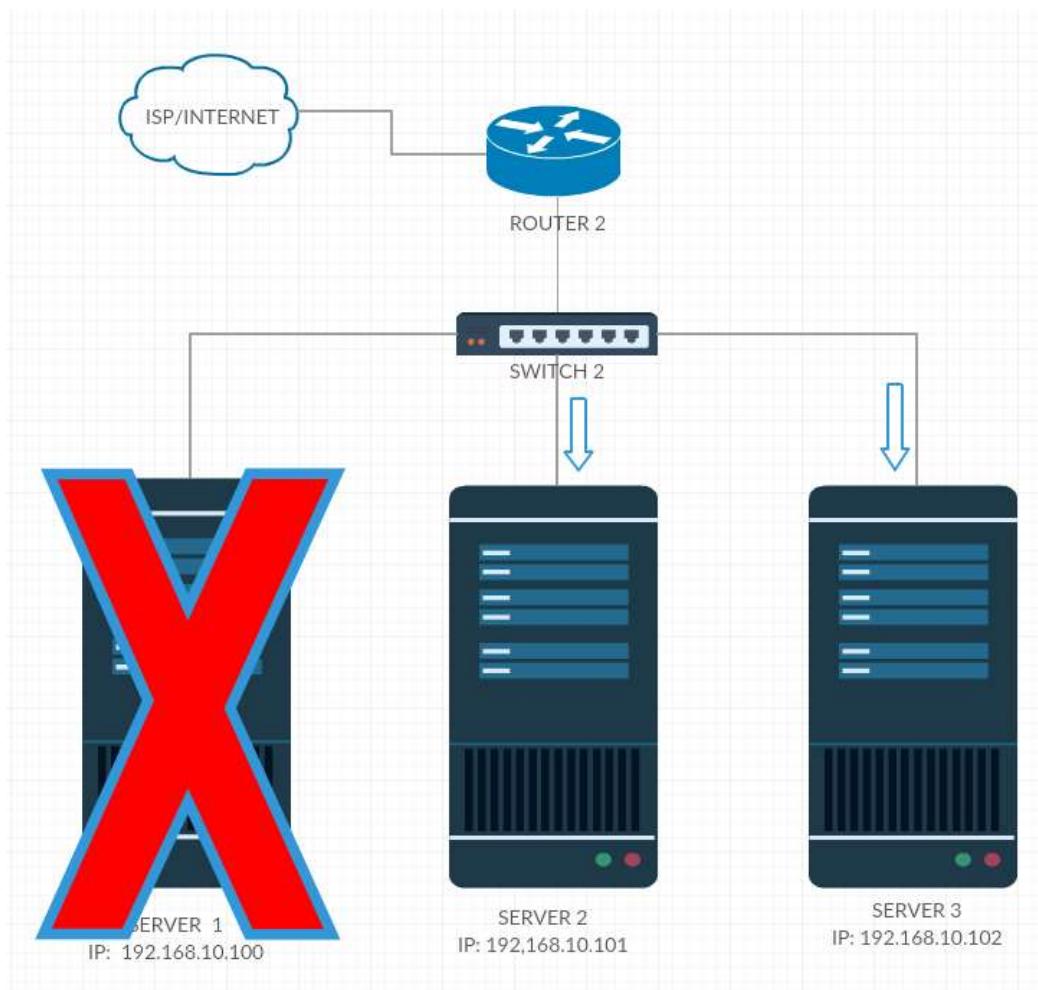


Figure 3-13

2.2 One of the router links is broken: The alternative router will be in use as shown in Case 1.1 and 1.2 or Figure 3-13 and 3-14. The same applies to if one of the switches is down.

3.4 Flowchart

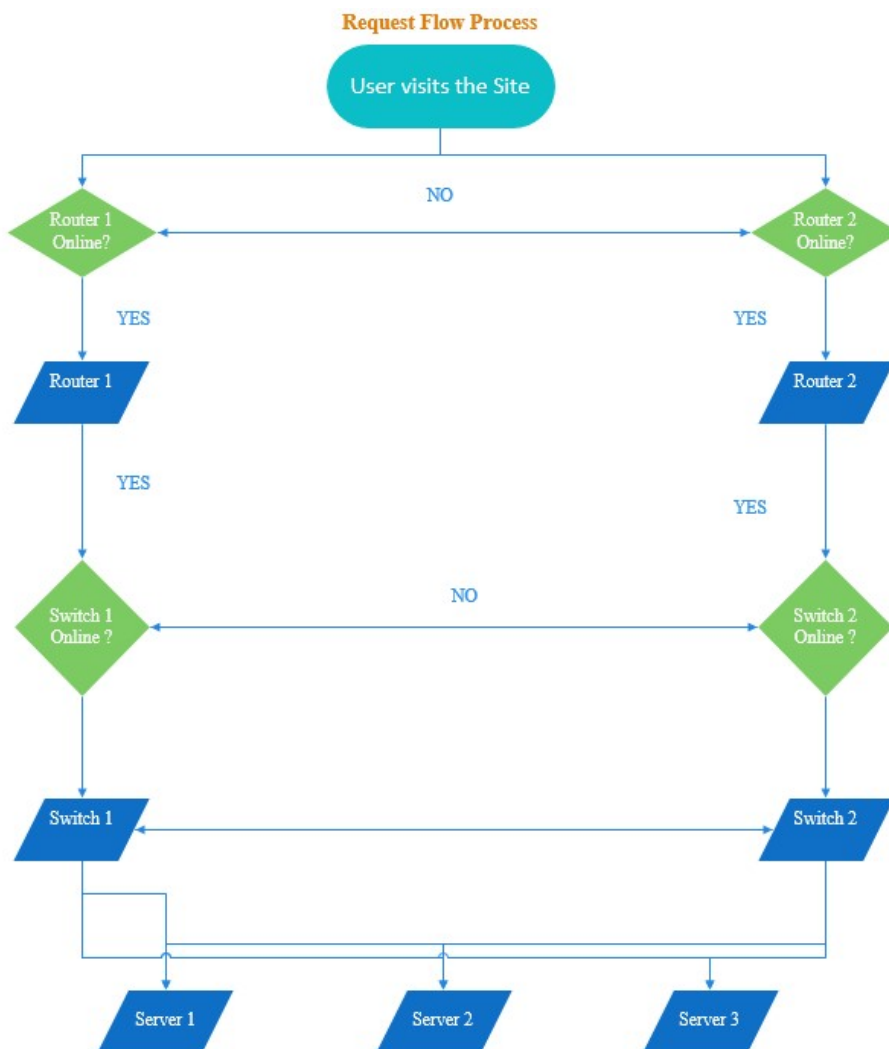


Figure 3-14 Request Flow Flowchart

CHAPTER 4 METHODOLOGY AND COST

4.1 Methodology and Approach Introduction

Since this is a project on network deployment and implementation, therefore PPDIIO lifecycle approach is used. PPDIIO means for prepare, plan, design, implement, create and optimize. The continuous life-cycle of services required for a network is defined by this methodology from Cisco.

Phases of PPDIIO

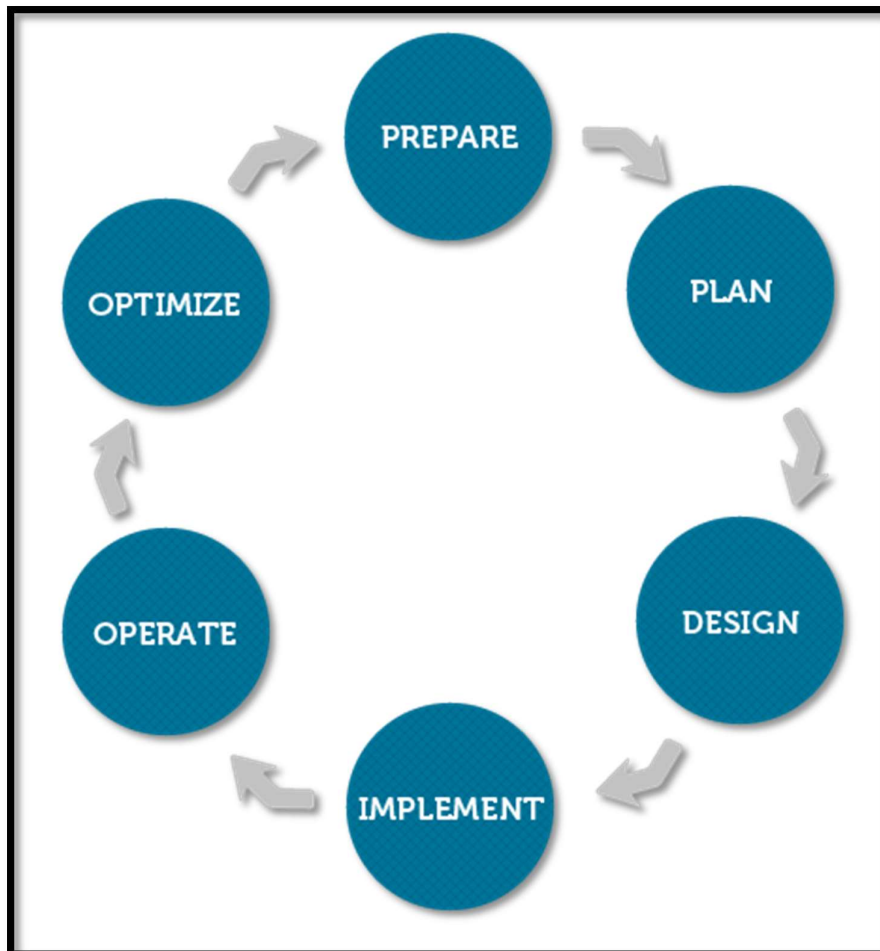


Figure 4-1 Phases of PPIDOO

Prepare	The network strategy is deployed and high-level conceptual architecture. Technologies are identified that can support this architecture.
Plan	Identify network requirements. Perform analysis on existing network and determine existing equipment or infrastructure that can support the proposed system.
Design	Draft of the network setup is drawn on planning software such as Visio Studio, Cisco Packet Tracer and GNS3.
Implement	The building process of the network is started.
Operate	Final test of the appropriateness of the design. Collecting data from data to day basis regarding performance for optimization phase.
Optimize	Proactive management of the network. Revise or adding configurations that can improve or solve the problems found in the operate phase.

Table 4-1 Brief description of each of the phases in PPDIIO

4.2 Cost Explanation

4.2.1 Pricing of Equipment and Devices

Table shows the prices of the equipment which required for the major approaches in Table 4-2. The equipment listed is mixture of all the equipment and devices needed. The price stated here is the price for the entry level devices / equipment.

Device / Equipment / Service	* Pricing in MYR
Barracuda Load Balancer 240 Appliance	8250.00
Barracuda Firewall X100	4650.00
Elastic SDN Pricing	435,600
12 pcs of 8m CAT 6 RJ 45 Network Cable	130.00
TP-LINK PCI Network Card 3 pcs	80.00
TP-LINK TL-SG1008D 8 Port Gigabit Switch 2 pcs	200.00
San Jose Cisco Secure IDS	35200
Cisco 1841 Router 2pcs	5500.00

Table 4-2 Pricing of the Equipment and Devices

4.2.2 Pricing of the Equipment or Devices Needed

Device / Equipment / Service	* Pricing in MYR
12 pcs of 8m CAT 6 RJ 45 Network Cable (Taobao, 2017)	130.00
TP-LINK PCI Network Card 3 pcs (Taobao, 2017)	80.00
TP-LINK TL-SG1008D 8 Port Gigabit Switch 2 pcs (Taobao, 2017)	200.00
Cisco 1841 Router 2pcs (Router-Switch.com,2017)	5500.00
Total Cost	5910.00

Table 4-3 Pricing of the Devices Used

Table 4-3 shows the prices of the devices used in this approach. This table only shows the price instead of the real cost incurred. Devices such as routers can be re-used if an organization already owned it.

However, the yellow highlighted rows in Table 6 are the devices must be purchase in order to implement the approaches mentioned in Table 1. By implementing this approach, the cost needed to purchase that equipment can be saved.

- The prices are inclusive of all hidden cost includes VAT/GST, tax and shipping charges.

CHAPTER 5 TESTING AND RESULTS OBTAINED

5.1 Testing Environment and Tools

5.1.1 Attack Tools

Denial of Service attack will be performing against the web servers by using Slowloris. Slowloris is a Perl script written by Robert RSnake where a single machine with minimal bandwidth enough to take down the web server without affecting other services. It initiates many connections to the target web server open and hold them as long as possible exhausting the concurrent connection pool by sending partial HTTP requests thus denying additional connection attempts from legitimate users. (*Slowloris*, no date). Solaris will connect to the target host with the interval of time t and the number of sockets s . The more sockets is used, the more packets it will send. The attack Slowloris used is asymmetric attack.

The command used to launch the attack is

. Slowloris.pl -dns -[IP/domain] -port [port number] -timeout [n] -num [k].

The relationship of n and k is launching using k number of sockets for every n seconds.

```
root@kali:~/Documents/ddos# ./Slowloris.pl -dns 192.168.237.60 -port 80 -timeout 1 -num 100
```

Figure 5-1 Command used to launch attack with time interval of 1 seconds with 100 sockets

Slowloris opens connections using the number of sockets and send HTTP Header to the server. The HTTP Header is shown in Figure 21. This is the partial HTTP request Slowloris sent.

```

my $primarypayload =
  "GET /$rand HTTP/1.1\r\n"
  . "Host: $sendhost\r\n"
  . "User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50313; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; MSOffice 12)\r\n"
  . "Content-Length: 42\r\n";
    
```

Figure 5-2 HTTP Header that Solaris send to the server

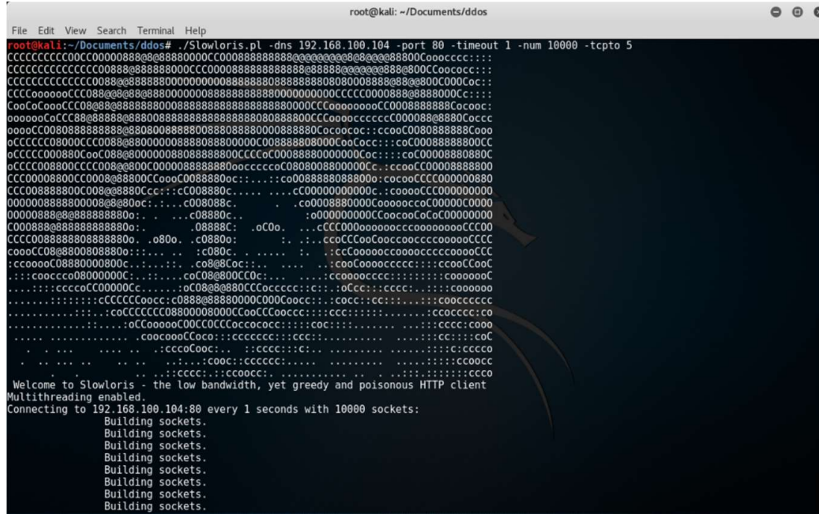


Figure 5-3 Interface of Slowloris

5.1.2 Testing Environment

The servers are serving HTTP requests and the website hosted is a self-coded resume website with only one jpg file need to be loaded. Figure 21 is the snapshot preview of the website hosted on each of the server.

The servers are running WAMP 3.0.6 with Apache 2.4.3 under Windows 7 Professional Operating System.

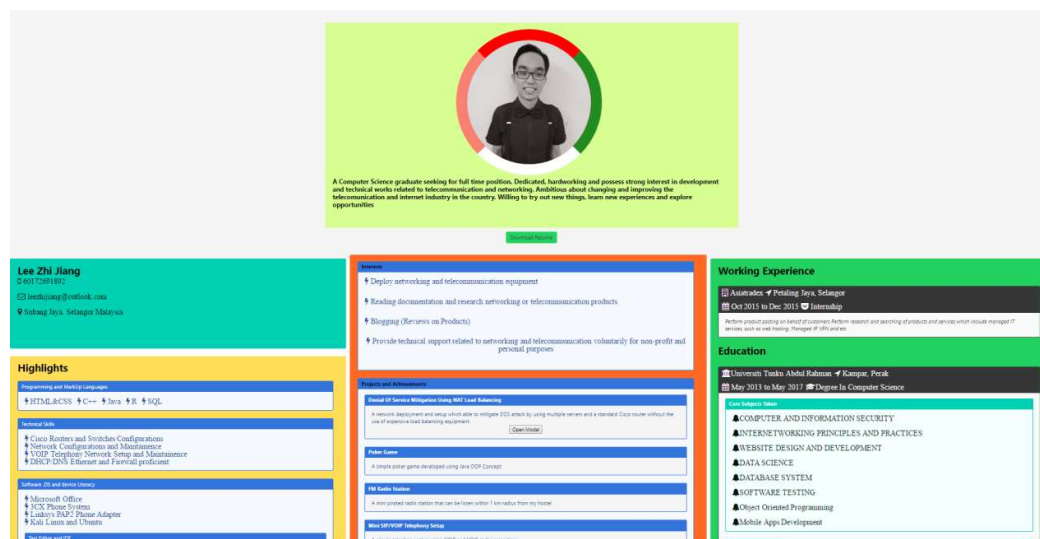


Figure 5-4 Snapshot of the website hoste

5.2 Test Plan

Test Number	Description of Test
1	<p>A typical setup without NAT Load Balancing. Just normal port forwarding.</p> <p>S0: Start with 80 as the number of sockets used.</p> <p>S1: Perform attack by using the public IP Address of the router.</p> <p>S2: Access the website using public IP of the router while the attack is going on. Record down is the website accessible or not.</p> <p>S3: Increment the number of sockets by 10.</p> <p>S4: Repeat S1 to S3, until the website is not accessible.</p> <p>S5: Record down the value x, where x is the number of sockets the website refused the connection or not accessible.</p>
2	<p>Setup with basic NAT Load Balancing as shown in Figure 3.</p> <p>S0: Start with x as the number of sockets used.</p> <p>S1: Perform attack by using the public IP Address of the router.</p> <p>S2: Access the website using public IP of the router while the attack is going on. Record down is the website accessible or not.</p> <p>S3: Increment the number of sockets by 150.</p>

	<p>S4: Repeat S1 to S3, until the website is not accessible.</p> <p>S5: Record down the value y_1, where y_1 is the number of sockets the website refused the connection or not accessible.</p>
3	<p>Using the completed network deployment as shown in Figure 2 with default fixed values of the worker module in MPM</p> <p>S0: Start with x as the number of sockets used.</p> <p>S1: Perform attack by using the public IP Address of the router.</p> <p>S2: Access the website using public IP of the router while the attack is going on. Record down is the website accessible or not.</p> <p>S3: Increment the number of sockets by 150.</p> <p>S4: Repeat S1 to S3, until the website is not accessible.</p> <p>S5: Record down the value y_2, where y_2 is the number of sockets the website refused the connection or not accessible.</p> <p>S6: Attempt to access by using Public IP of another router. Record down whether is it still accessible or not.</p>
4	<p>Using the completed network deployment as shown in Figure 2 with dynamic values of the worker module in MPM</p> <p>S0: Start with y_2 as the number of sockets used and 200 as the value of $\text{MaxRequestWorkers}, j$ for all the servers.</p> <p>S1: Perform attack by using the public IP Address of the router.</p> <p>S2: Access the website using public IP of the router while the attack is going on. Record down is the website accessible or not.</p> <p>S3: Increment the number of sockets by 300.</p> <p>S4: Repeat S1 to S3, until the website is not accessible.</p> <p>S5: Record down the value t, where t is the number of sockets the website refused the connection or not accessible.</p> <p>S6: Increment the values of j by 100 for all the servers.</p> <p>S7: Set the number of socket to the value of t.</p> <p>S8: Repeat S1 to S7 until the value of j is at 1000.</p>

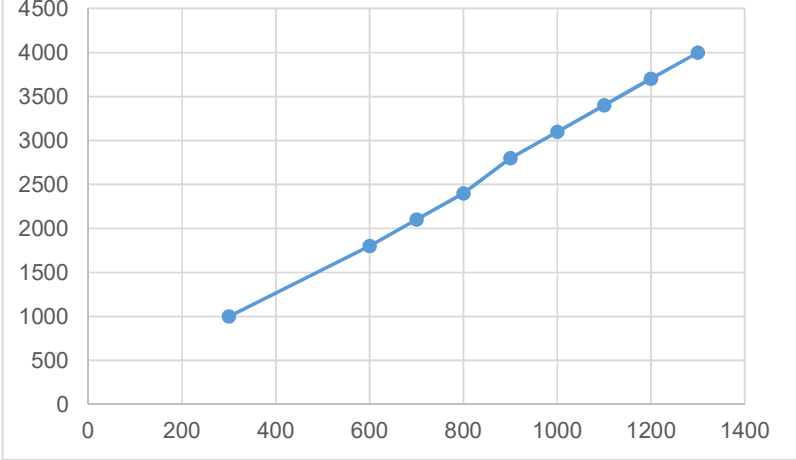
5	Using the completed network deployment as shown in Figure 2 with fixed values of the worker module in MPM as stated in Table 4. S0: Start with t as the number of sockets used. S1: Perform attack by using the public IP Address of the router. S2: Access the website using public IP of the router while he attacks is going on. Record down is the website accessible or not. S3: Increment the number of sockets by 500. S4: Repeat S1 to S3, until the website is not accessible. S5: Record down the value k , where k is the number of sockets the website refused the connection or not accessible
6	Disable one of the device and access the website from another router

Table 5-1 Descriptions of Tests

Browser cache will affect the results since it stores the copy of the visited websites. Therefore, a new private browsing window is used for every round of test on website loading.

5.3 Expected Results

Test Case	Description of Results	
1	<p>From the observation, the website able to load in less than 15 seconds for s value from 100 -140. The website is not accepting connection request anymore when the s value is above 150.</p>	
	Number of Sockets Used	Is the Website Still Accessible?
	80	Yes
	100	Yes
	120	Yes
	140	Yes
	160	No
2	<p>With NAT Load Balancing implemented, legitimate user still able to access the website as illustrated in Figure 5-6 when the number of sockets per seconds is up to 800. At value of 900 and above, only Figure 5-5 will be shown. Although the number is varying from time to time but with reference to the setup without NAT Load Balancing, the setup with load balancing can hold at least 400 % more connections in average.</p>	
	Number of Sockets Used	Is the Website Still Accessible?
	50	Yes
	100	Yes
	200	Yes
	300	Yes
	400	Yes
	500	No
	600	No
	700	No

3	Same Result in Test 2. Unable to access from another router.																				
4	<table border="1" data-bbox="509 302 1330 919"> <thead> <tr> <th data-bbox="509 302 919 359">Max Request Worker, j</th> <th data-bbox="919 302 1330 359">Number of Sockets Used, t</th> </tr> </thead> <tbody> <tr> <td data-bbox="509 359 919 420">300</td> <td data-bbox="919 359 1330 420">1000</td> </tr> <tr> <td data-bbox="509 420 919 480">600</td> <td data-bbox="919 420 1330 480">1800</td> </tr> <tr> <td data-bbox="509 480 919 541">700</td> <td data-bbox="919 480 1330 541">2100</td> </tr> <tr> <td data-bbox="509 541 919 602">800</td> <td data-bbox="919 541 1330 602">2400</td> </tr> <tr> <td data-bbox="509 602 919 663">900</td> <td data-bbox="919 602 1330 663">2800</td> </tr> <tr> <td data-bbox="509 663 919 724">1000</td> <td data-bbox="919 663 1330 724">3100</td> </tr> <tr> <td data-bbox="509 724 919 785">1100</td> <td data-bbox="919 724 1330 785">3400</td> </tr> <tr> <td data-bbox="509 785 919 846">1200</td> <td data-bbox="919 785 1330 846">3700</td> </tr> <tr> <td data-bbox="509 846 919 919">1300</td> <td data-bbox="919 846 1330 919">4000</td> </tr> </tbody> </table> <div data-bbox="509 1037 1300 1577"> <p style="text-align: center;">Graph of t vs j</p>  </div>	Max Request Worker, j	Number of Sockets Used, t	300	1000	600	1800	700	2100	800	2400	900	2800	1000	3100	1100	3400	1200	3700	1300	4000
Max Request Worker, j	Number of Sockets Used, t																				
300	1000																				
600	1800																				
700	2100																				
800	2400																				
900	2800																				
1000	3100																				
1100	3400																				
1200	3700																				
1300	4000																				
5																					

	Number of Sockets Used	Is the Website Still Accessible?
	1000	Yes
	2000	Yes
	3000	Yes
	4000	Yes
	5000	Yes
	6000	Yes
	7000	Yes
	8000	Yes
	9000	Yes
	10000	Yes
6	Website is still accessible	

Table 5-2 Overall Results Tabulation

5.4 Result Discussions and Problem Solving

Table 5-2 illustrate the expected result of this project, however after tests are performed using the steps in Table 5-1 only **Test Case 1 to Test Case 3** are accurate. The websites are not accessible with the attack using 450 sockets eventhough the values in the mpm worker module are set to the highest. The reasons behind is because Apache is hosted in Windows 7 which is categorized under Windows NT family. The above configuration is **only valid for Linux based Apache server**.

In order to make Apache to spawn more threads the *mpm_winnt_module* should be configured by increasing the values of threads per child in order to allow the server to respond to more requests.

The number of sockets used is also equivalent to the value of threads per child multiply with the number of servers used for load balancing. In the setup, 3 servers are used, that is the reasn why the website is not accessible anymore when the number of sockets used is more than or equivalent to 450 where as the setup with no port

forwarding need 150 sockets to successfully cause Denial of Service to the server. The default value of the number of threads is 150 therefore it cannot served more than 150 requests simultaneously in one second. This can be proven by using the error log generated by Apache server.

```
[Fri Apr 07 14:37:17.633897 2017] [mpm_winnt:notice] [pid 3172:tid 160] AH00354: child: Starting 150 worker threads.
[Fri Apr 07 14:39:42.152551 2017] [mpm_winnt:error] [pid 3172:tid 4652] AH00326: Server ran out of threads to serve requests. Consider raising the ThreadsPerChild setting
[Fri Apr 07 15:00:52.787584 2017] [mpm_winnt:notice] [pid 3596:tid 336] AH00422: Parent: Received shutdown signal -- shutting down the server.
[Fri Apr 07 15:00:54.815588 2017] [mpm_winnt:notice] [pid 3172:tid 160] AH00364: child: All worker threads have exited. ...
```

Figure 5-5 Error message regarding insufficient threads to serve requests

Figure 5 – 5 is part of the screenshot that proved the module that is responsible for the spanning of threads is mpm_winnt module instead of mpm_worker_module because the server is running under Windows operating system. Therefore by increasing the value of ThreadsPerChild the server able to serve more requests.

```
# winNT MPM
# ThreadsPerChild: constant number of worker threads in the server
process
# MaxConnectionsPerChild: maximum number of connections a server process
serves
<IfModule mpm_winnt_module>
    ThreadsPerChild    600
    MaxConnectionsPerChild    0
</IfModule>
```

Figure 5-6 WinNT MPM Configuration Section

Figure 5-6 illustrate the WinNT MPM Configuration that should be implemented instead of the mpm_worker module that only applicable in Linux operating system. The values stated in the Figure is the final value set for moderate level of Denial of Service mitigation as the server can still continue to serve request even when the attack I generated using more than 30,000 sockets per second. The result is represented under Test 5 of Table 5-4.

Denial of Service attack is able to be mitigated by using NAT Load Balancing and the use of multithreading as enhancement. However according to the results, multithreading is the key method to improve the situation during a Denial of Service Attack. By modifying configuration file to allow multithreading, the server is tuned to spawn more resources to serve the requests thus mitigated the attempt of Denial of

Service attack.

Redundancy is implemented by adding one extra router also improves the situation whereby the service can still be accessed from another router. This proven that the hypothesis that the servers are the bottleneck is wrong. In fact, the bottleneck in the network will vary as time passed by. It will change from one device to another as we upgrade or improved the device which is the bottleneck.

All the devices including router has their own connection pool or resources. As soon as the resources is exhausted, legitimate user will not able to access the website and will be greeted with error message in their browser as shown in Figure 5-7.

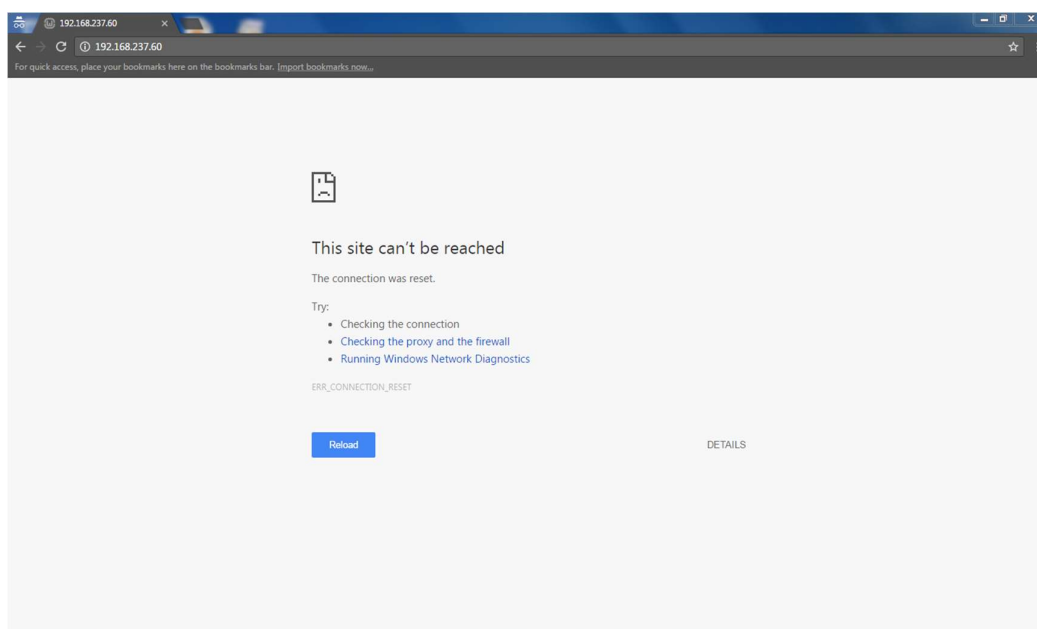


Figure 5-7 Error Message when legitimate trying to access site under DOS Attack

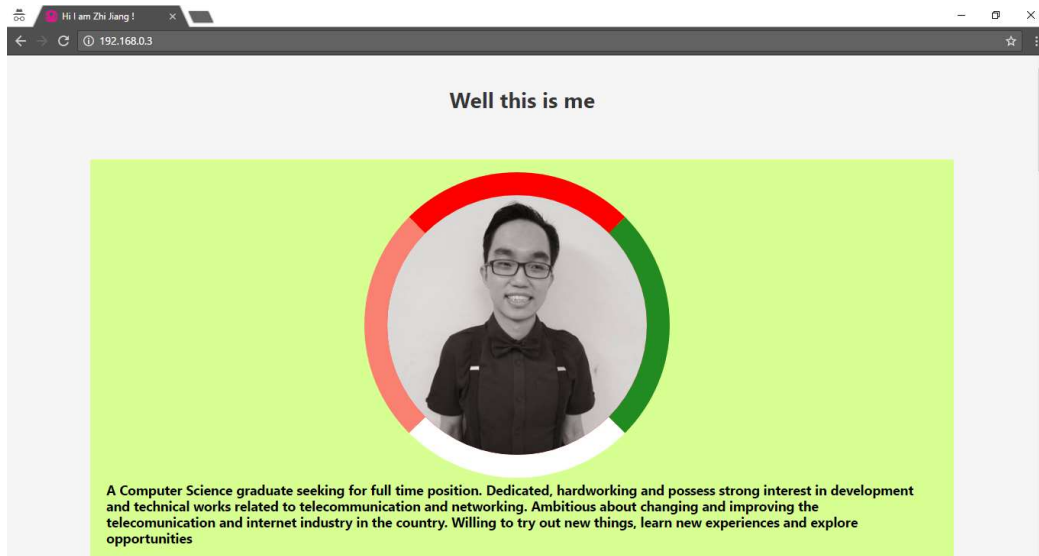


Figure 5-8 Legitimate User Should Able to see this page if the website able to load

Figure 5-8 illustrate the screen that will able to see by legitimate user if the website is able to load. (The web server able to respond and served the request)

CHAPTER 6 CONCLUSION

6.1 Project Review and Summary

NAT Load Balancing is implemented in this project to mitigate Denial of Service attack. NAT Load Balancing is also known as TCP Load Distribution which forwards packets or requests to more than one devices or servers in a round-robin basis. By distributing load in a round-robin basis, all the devices or servers will share the load hence making each of them more resilient to huge amount of requests.

NAT Load Balancing coupled with multi-devices and multi-threading making the entire project to become a low cost yet effective in mitigating Denial of Service Attack. Besides, the entire project implementation also capable of handling larger requests or traffic hence reducing the probability the services will go offline due to huge requests.

In a nutshell, this project meets the expectations because all the objectives are achieved. During the project implementation, there are several issues with the router such as it went into recovery mode after factory reset failure, unable to save running configuration and etc. However, all of them able to be solved in a quick manner due to easily access guidelines and documentation from Cisco.

NAT Load Balancing should be considered by website owners or organization as one of the way to mitigate Denial of Service or Distributed Denial of Service Attack because it is cost effective and easily manageable.

6.2 Future Works and Improvements

Although this is a successful project, however there are still a lot more rooms for improvement to further improve the efficiency and the robustness of the entire network.

First of all, more servers or PCs can be added into the network to serve the requests. By adding more devices, each device will share a smaller load hence making the entire network more efficient.

From developer point of view, the firmware of the routers and be changed into a custom one. It is possible to re-write the algorithms to make the router able to make smart decisions to forward the packets dynamically. Dynamically means the router will use different ways on different situations.

In order to convince more people to use this network implementation, this project also should try with managed routers from other manufacture to prove that this setup in device friendly and applicable in major environment.

Works Cited

- Apache. (2017). *Apache MPM worker*. Retrieved March 15, 2017, from <http://httpd.apache.org/docs/2.4/mod/worker.html>
- ARBOR Networks. (2013). *DDoS Mitigation Best Practices*. Retrieved August 11, 2016, from https://www.arbornetworks.com/images/documents/Arbor%20Insights/AI_DD_oSMitigation_EN2013.pdf
- B. B. Gupta, S. M. (2010). Distributed Denial of Service Prevention Technique. *International Journal of Computer and Electrical Engineering*, 2(2), 268-276.
- Barracuda Firewall X - Information, Pricing and Ordering*. (n.d.). Retrieved March 20, 2017, from Ntsecurity.com: <http://www.ntsecurity.com/barracuda-products/firewall-x.html>
- Barracuda Load Balancer - Information, Pricing and Ordering*. (n.d.). Retrieved March 21, 2017, from Ntsecurity.com: <http://www.ntsecurity.com/barracuda-products/barracuda-load-balancer.html>
- Big Switch Network. (n.d.). *Elastic SDN Pricing*. Retrieved March 21, 2017, from <http://go.bigswitch.com/rs/974-WXR-561/images/Elastic%20SDN%20Pricing%20Overview.pdf>
- Davis, B. (2010). Leveraging the Load Balancer to Fight DDoS . *SANS Institute InfoSec Reading Room*.
- F5 Networks Inc. (n.d.). *Glossary and Terms : Load Balancer*. Retrieved August 10, 2016, from <https://f5.com/glossary/load-balancer>
- Gates, S. (2013). DDoS ATTACKS: MOTIVES, MECHANISMS AND MITIGATION. Retrieved from https://www.rsaconference.com/writable/presentations/file_upload/sec-w04_final.pdf
- Geer, D. (n.d.). *Five reasons IT pros are not ready for SDN investment*. Retrieved August 10, 2016, from <http://searchsdn.techtarget.com/feature/Five-reasons-IT-pros-are-not-ready-for-SDN-investment>
- HAProxy. (2012). *USE A LOAD-BALANCER AS A FIRST ROW OF DEFENSE AGAINST DDOS*. Retrieved August 10, 2016, from <http://blog.haproxy.com/2012/02/27/use-a-load-balancer-as-a-first-row-of-defense-against-ddos/>
- Internet-Computer-Security.com. (n.d.). *IPS (Intrusion Prevention System) and IDS (Intrusion Detection Systems)*. Retrieved August 9, 2016, from Internet-Computer-Security.com: <http://www.internet-computer-security.com/Firewall/IPS.html>
- Kenig, R. (2013). *Can your firewall and IPS block DDOS Attacks ?* Retrieved August 10, 2016, from <https://blog.radware.com/security/2013/05/can-firewall-and-ips-block-ddos-attacks/>
- Kiggins, A., & Lyon, J. (2016). AWS Best Practices for DDoS Resiliency. Amazon Web

- Services. Retrieved from https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf
- MATTHEWS, T. (2014). *Incapsula Survey: What DDOS Attacks really cost Business*. Incapsula. Retrieved from <http://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf>
- MPM or Multi Processing Module - How to LAMP*. (n.d.). Retrieved March 18, 2017, from <http://howtolamp.com/lamp/httpd/2.4/configuration-files/>
- Nayana Y, M. G. (2015). DDoS Mitigation using Software Defined Network. *International Journal of Engineering Trends and Technology*, 24(5), 258-264.
- Palo Alto Networks, Inc. (2014). *Application DDoS Mitigation*. Palo Alto Networks. Retrieved August 11, 2016, from <https://live.paloaltonetworks.com/t5/Documentation-Articles/Application-DDoS-Mitigation/ta-p/54531?attachment-id=230>
- Radware, Ltd. (2013). *Approaches to Mitigate DDoS Attacks Whitepaper*. Radware. Retrieved from <http://www.infosec-cloud.com/wp-content/uploads/2015/06/premises-or-cloud-hybrid-ddos-mitigation-wp.pdf>
- Turnbull, M. (n.d.). *Simple Denial Of Service DOS Attack Mitigation Using HAProxy*. Retrieved August 8, 2016, from <http://loadbalancer.org/blog/simple-denial-of-service-dos-attack-mitigation-using-haproxy-2>
- Villanueva, J. C. (2015). *Comparing Load Balancing Algorithms*. Retrieved August 10, 2016, from Managed File Transfer Solutions: <http://www.jscape.com/blog/load-balancing-algorithms>
- 栖麟数码专营店. (2017). *P-LINK TL-SG1008D 8口千兆交换机 千兆钢壳1000M网络监控交换机-tmall.com 天猫*. Retrieved March 20, 2017, from Taobao: <https://world.tmall.com/item/45541598034.htm?spm=a312a.7700714.0.0.K73X21>
- 赢为电器旗舰店. (2017). *赢为 cat6 网线 纯铜千兆扁平六类网线 室内网络宽带线 1/5/10/30 米-tmall.com 天猫*. Retrieved March 20, 2017, from Taobao: <https://world.tmall.com/item/39998870176.htm?spm=a312a.7700714.0.0.POLan4&skuId=57322210452>

APPENDIX A Running Config of Router 1

```
ZJ#show run
Building configuration...

Current configuration : 4398 bytes
!
version 12.4
service config
service timestamps debug datetimemsec
service timestamps log datetimemsec
no service password-encryption
!
hostname ZJ
!
boot-start-marker
boot-end-marker
!
no logging buffered
enable secret 5 $1$He1h$yJ9HU68nxf1i0xDE1Gv07.
enable password csc
!
no aaa new-model
ipcef
!
!
no ipdhcp use vrf connected
ipauth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
!
!
!
!
interface FastEthernet0/0
  description $FW_OUTSIDE$
ip address dhcp
ipnat outside
```

```
ip virtual-reassembly
  duplex auto
  speed auto
  service-policy output SDM-QoS-Policy-1
!
interface FastEthernet0/1
  description $FW_INSIDE$
ip address 192.168.10.254 255.255.255.0
ipnat inside
ip virtual-reassembly
  duplex auto
  speed auto
  no mop enabled
!
interface Serial0/0/0
  no ip address
  shutdown
  no fair-queue
  clock rate 2000000
!
interface Serial0/0/1
  no ip address
  shutdown
  clock rate 2000000
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ipnat pool ROTATE 192.168.10.1 192.168.10.3 prefix-length 24 type rotary
ipnat inside source list 11 interface FastEthernet0/0 overload
ipnat inside destination list LOADBALANCE pool ROTATE
!
ip access-list extended LOADBALANCE
  permit tcp any host 192.168.237.60 eq www
  permit tcp any host 192.168.237.61 eq www
  permit tcp any host 192.168.237.62 eq www
  permit tcp any host 192.168.237.63 eq www
  permit tcp any host 192.168.237.64 eq www
  permit tcp any host 192.168.237.65 eq www
  permit tcp any host 192.168.237.0 eq www
```

```
!  
access-list 11 permit 192.168.10.0 0.0.0.255  
access-list 100 remark SDM_ACL Category=128  
access-list 100 permit ip host 255.255.255.255 any  
access-list 100 permit ip 127.0.0.0 0.255.255.255 any  
access-list 101 remark SDM_ACL Category=0  
access-list 101 permit ip any host 192.168.10.1  
dialer-list 1 protocol ip permit  
!  
!  
!  
control-plane  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
    password cisco  
    login  
!  
scheduler allocate 20000 1000  
end
```



```
!  
!  
  
interface FastEthernet0/0  
ip address dhcp  
ipnat outside  
ip virtual-reassembly  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
ip address 192.168.10.253 255.255.255.0  
ipnat inside  
ip virtual-reassembly  
duplex auto  
speed auto  
no mop enabled  
!  
interface Serial0/0/0  
no ip address  
shutdown  
clockrate 125000  
!  
interface Serial0/0/1  
no ip address  
shutdown  
clockrate 125000  
!  
ip classless  
!  
no ip http server  
no ip http secure-server  
ipnat pool ROTATE 192.168.10.1 192.168.10.3 prefix-length 24  
type rotary  
ipnat inside source list 11 interface FastEthernet0/0 overload  
ipnat inside destination list LOADBALANCE pool ROTATE  
!  
ip access-list extended LOADBALANCE  
permit tcp any host 192.168.0.4 eq www  
permit tcp any host 192.168.0.5 eq www  
permit tcp any host 192.168.0.6 eq www  
permit tcp any host 192.168.0.7 eq www
```



```
!  
access-list 11 permit 192.168.10.0 0.0.0.255  
!  
!  
!  
!  
control-plane  
!  
!  
!  
!  
!  
!  
!  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
  login  
!  
end
```

APENDIX C BIWEEKLY REPORTS

FINAL YEAR PROJECT BIWEEKLY REPORT

(Project I / Project II)

Trimester, Year: Y3 T3	Study week no.: 1,2
Student Name & ID: LEE ZHI JIANG 1303624	
Supervisor: DR GAN MING LEE	
Project Title: DENIAL OF SERVICE MITIGATION BY USING NAT LOAD BALANCING	

1. WORK DONE

- Setting up devices: 3 routers, 6 switches and servers
- Performing VLAN on switches to act as virtual port
- Study and attempting to perform double NAT and double TCP Load Distribution

2. WORK TO BE DONE

- . Research on alternatives not to use too many switches

3. PROBLEMS ENCOUNTERED

- Unable to perform double TCP Load Distribution

4. SELF EVALUATION OF THE PROGRESS

-

Supervisor's signature

Student's signature

Trimester, Year: Y3 T2	Study week no.: 3,4
Student Name & ID: LEE ZHI JIANG 1303624	
Supervisor: DR GAN MING LEE	
Project Title: DENIAL OF SERVICE MITIGATION BY USING NAT LOAD BALANCING	

<p>1. WORK DONE</p> <ul style="list-style-type: none"> - Redesign network to use only 2 routers and 2 switches - Factory reset all the routers and switches - Redo the setup using only 2 routers and 2 switches - Perform NAT configurations on both the routers
<p>2. WORK TO BE DONE</p> <ul style="list-style-type: none"> - Study on multithreading on Apache. - Study and figure out advance configurations on Apache - Apache documentation reading
<p>3. PROBLEMS ENCOUNTERED</p> <ol style="list-style-type: none"> 1. Router entering recovery mode. 2. Unable to save running config
<p>4. SELF EVALUATION OF THE PROGRESS</p> <ul style="list-style-type: none"> - The progress is too fast

Supervisor's signature

Student's signature

Trimester, Year: Y3 T2	Study week no.: 5,6
Student Name & ID: LEE ZHI JIANG 1303624	
Supervisor: DR GAN MING LEE	
Project Title: DENIAL OF SERVICE MITIGATION BY USING NAT LOAD BALANCING	

<p>1. WORK DONE</p> <ol style="list-style-type: none"> 1. Reinstall WAMP and Apache on the computers 2. Perform TCP Load Distribution configurations on the routers 3. Testing to validate the configuration 4. Performing Single Point of Failure test
<p>2. WORK TO BE DONE</p> <p>None</p>
<p>3. PROBLEMS ENCOUNTERED</p> <p>None</p>
<p>4. SELF EVALUATION OF THE PROGRESS</p> <p>None</p>

Supervisor's signature

Student's signature

Trimester, Year: Y3 T2	Study week no.: 7,8
Student Name & ID: LEE ZHI JIANG 1303624	
Supervisor: DR GAN MING LEE	
Project Title: DENIAL OF SERVICE MITIGATION BY USING NAT LOAD BALANCING	

<p>1. WORK DONE</p> <ol style="list-style-type: none"> 1. Modifying Apache configuration files to enhance multithreading 2. Performing Denial of Service mitigation tests using different values in the Apache configuration files (mpm-worker) 3. Report Compilation 4. Study on spanning tree protocol 5. Apache documentation reading 6. Change the content of the website hosted on the servers
<p>2. WORK TO BE DONE</p> <p>None</p>
<p>3. PROBLEMS ENCOUNTERED</p> <p>It is difficult to understand the configuration files in the first place.</p>
<p>4. SELF EVALUATION OF THE PROGRESS</p> <p>None</p>

Supervisor's signature

Student's signature

Trimester, Year: Y3 T2	Study week no.: 9,10
Student Name & ID: LEE ZHI JIANG 1303624	
Supervisor: DR GAN MING LEE	
Project Title: DENIAL OF SERVICE MITIGATION BY USING NAT LOAD BALANCING	

<p>1. WORK DONE</p> <ol style="list-style-type: none">1. Study on the pricing and cost of implementation2. Research on prices of networking devices3. Perform different test cases as shown in the report.4. Report Compilation
<p>2. WORK TO BE DONE</p> <p>Proof reading parts on the written report.</p>
<p>3. PROBLEMS ENCOUNTERED</p> <p>None</p>
<p>4. SELF EVALUATION OF THE PROGRESS</p> <p>Progress is on track.</p>

Supervisor's signature

Student's signature

POSTER

INTRODUCTION


Organization face DOS attacks frequently and at the same time need to cater huge number of requests. Purchasing a load balancing device is too costly and can be unnecessary but traditional methods such as firewall doesn't serve the effect. However, organization will suffer huge loss if nothing is implemented

DISCUSSIONS

This method is succesful because it as the feature of load sharing, fail over and utilization of multithreading to create more resources to serve those huge incomming requests

STARTER PACK FOR DENIAL OF SERVICE MITIGATION

DENIAL OF SERVICE ATTACK



M I T I G A T I O N **U S I N G**

NAT LOAD BALANCING

COST EFFECTIVE + EASY ADMINISTRATION + GOOD PERFORMANCE

METHODS

By implementing TCP Load Distribution on the router the requests can be distributed across all the devices in round robin basis thus reducing the chances of overloading a particular device.


Adding an additional router and switch to create a second network with tcp load distribution able to act as fail over in case one of the router fails

RESULTS

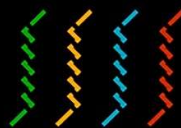
Normal Port Forwarding vs this method


Port Forwarding	This Method
140	8000
	with Minimum multithreading
SCORE	SCORE

LITTLE HELPER



MULTITHREADING





LEE ZHI JIANG
DR GAN MING LEE

TURNITIN PLAGARISM CHECK RESULT



Turnitin Originality Report

DENIAL OF SERVICE ATTACK
MITIGATION USING NAT LOAD
BALACING by Zhi Jiang Lee

From FYP2 Turnitin Jan2017 (FYP2
Turnitin Jan2017)

Similarity Index	Similarity by Source
7%	Internet Sources: 5% Publications: 2% Student Papers: 4%

Processed on 28-Mar-2017 15:05 MYT

ID: 790563045

Word Count: 8477

sources:

- 1 1% match (Internet from 16-Nov-2014)
<http://searchsdn.techtarget.com/feature/Five-reasons-IT-pros-are-not-ready-for-SDN-investment>
- 2 1% match (Internet from 20-Jul-2016)
<https://www.scribd.com/document/232768290/Httpd-Docs-2-4-9-En>
- 3 1% match (publications)
[B. B. Gupta, "Defending against Distributed Denial of Service Attacks: Issues and Challenges". Information Security Journal A Global Perspective, 2009](#)
- 4 1% match (Internet from 19-Jun-2015)
<http://www.secdist.se/2013/05/can-your-firewall-and-ips-block-ddos-attacks/>
- 5 < 1% match (Internet from 02-Jun-2013)
http://www.arbornetworks.com/docman-component/doc_download/609-ddos-
- 6 < 1% match (student papers from 26-Mar-2014)
[Submitted to Middlesex University on 2014-03-26](#)
- 7 < 1% match (student papers from 13-Oct-2016)
[Submitted to Webster University on 2016-10-13](#)
- 8 < 1% match (student papers from 21-Jun-2010)
[Submitted to Middlesex University on 2010-06-21](#)
- 9 < 1% match (student papers from 28-Dec-2016)
[Submitted to Western Governors University on 2016-12-28](#)
- 10 < 1% match (Internet from 08-Aug-2013)
<http://luckysport.ru/devid-hei-zavershit-kareru-v-2011-godu.html>

Turnitin Document Viewer - Google Chrome

Secure | https://turnitin.com/dv?o=790563045&u=1058145422&s=&student_user=1&lang=en_us

FYP2 Turnitin Jan2017 FYP2 Turnitin Jan2017 - DUE 30-Jun-20-

Originally GradeMark PeerMark DENIAL OF SERVICE ATTACK MITIGATION USING turnitin 7% SIMILAR OUT OF 9 --

Match Overview

Match Number	Source	Similarity
1	searchsdn.techtarget.c... Internet source	1%
2	www.scribd.com Internet source	1%
3	B. B. Gupta. "Defendin... Publication	1%
4	Submitted to Middlesex... Student paper	1%
5	www.secdlist.se Internet source	1%
6	www.arbornetworks.com Internet source	<1%
7	Submitted to Webster U.. Student paper	<1%
8	Submitted to Western ... Student paper	<1%
9	luckysport.ru Internet source	<1%
10	Submitted to Sabanci U.. Student paper	<1%
11	Submitted to Tezpur Un.. Student paper	<1%
12	www.fullwood.tv Internet source	<1%
13	htpd.apache.org Internet source	<1%

Usually botnets are involved in this attack. However, it is a different story for asymmetric attack, the attacker just need to make use of some internet protocol to send a relatively small amount of data but able to trigger a large reply from the victim side which resulted in huge consumption of critical resources which will cause failure.

This paper organized as follows. The first chapter contains brief explanation about Denial of Service. The explanation includes types, causes, impact and challenges faced by organization in handling DOS attack. Next, is on my proposed approach in mitigating the attack with the objectives and achievements. Chapter 2 is about reviews on the current available ways and methods to handle Denial of Service attack. The next few chapters is about the explanations about the network deployment and configurations, methodology, testing plans and methods and results. The last chapter concludes this paper by making a general conclusion which contains about the author personal insight and experience on the process of producing this paper.

1.0.2 DDOS Attack Reasons (ARBOR NETWORKS, 2013):

Besides the decrease in the cost of technologies, there are still several factors that contributed to the increase in DDOS attacks. ARBOR Networks also discussed a few in one of their publication is 2013. "It is not just financial institutions and gaming sites which are being targeted, we have seen government departments hit, e-commerce sites and even pizza delivery companies being targeted. Why this change? Well, there are a number of reasons" (ARBOR NETWORKS, 2013).

Two out of three reasons are chosen to highlight here:

1. Attack tools are easily to be downloaded online: The tools available online can be downloaded and used by anyone therefore any person or organization or even state that is looking for a way to impact other internet

PAGE: 2 OF 48

Text-Only Report

Universiti Tunku Abdul Rahman			
Form Title : Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1 of 1



FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	
ID Number(s)	
Programme / Course	
Title of Final Year Project	

Similarity	Supervisor's Comments (Compulsory if parameters of originality exceeds the limits approved by UTAR)
Overall similarity index: _____ % Similarity by source Internet Sources: _____ % Publications: _____ % Student Papers: _____ %	
Number of individual sources listed of more than 3% similarity: _____	
Parameters of originality required and limits approved by UTAR are as Follows: (i) Overall similarity index is 20% and below, and (ii) Matching of individual sources listed must be less than 3% each, and (iii) Matching texts in continuous block must not exceed 8 words <i>Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.</i>	

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

Signature of Supervisor

Signature of Co-Supervisor

Name: _____

Name: _____

Date: _____

Date: _____