

DENIAL OF SERVICE ATTACK MITIGATION USING NAT LOAD BALACING

BY

LEE ZHI JIANG

A PROPOSAL

SUBMITTED TO

UNIVERSITI TUNKU ABDUL RAHMAN

In partial fulfillment of the requirements

For the degree of

BACHELOR OF COMPUTER SCIENCE (HONS)

Faculty of Information Communication Technology

(Perak Campus)

OCTOBER 2016

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 : _____

Name : _____

Date : _____

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 able to mitigate the attack by allowing the service to stay online for a longer period. Routers with NAT Load Balancing configurations 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. Besides, it is also cost effective because this deployment emphasizes on the concept of reuse.

Table of Contents

DECLARATION OF ORIGINALITY	1
ABSTRACT	2
List of Tables	4
List of Figures	5
List of Symbols	6
List of Abbreviations	7
CHAPTER 1	8
1.0 Introduction	8
1.1 Problems related to DDOS	9
1.1.2 Organization Preparation and Readiness Against DDOS Attacks	9
1.1.1 Business Impact on DDOS (Tim Matthews, n. d)	9
1.1.3 Traditional Network Security Solutions Cannot Mitigate DDOS (Radware, 2013)	10
1.1.4 Deploying anti DDOS device can be costly and difficult	10
1.2 Project Scope	11
1.4 Project Innovation and Contribution	12
1.5 Background Information	12
CHAPTER 2 LITERATURE REVIEW	14
2.1 Firewall, IPS, IDS (IPS and IDS, 2011; Kening, 2013)	14
2.2 Mitigation using SDN (Nayana et al. 2015)	16
2.3 Cloud Services (Radware, 2013)	17
2.4 Other General Techniques (Gupta, 2010)	18
CHAPTER 3 PROPOSED METHOD AND APPROACHES	20
3.0 Methods/ Technologies Involved	20
3.1 System Design /Overview	22
3.2 Testing and Evaluation Descriptions with Results for First Part of Project	26
3.4 Implementation Issue and Challenges	29
3.5 Timeline	30
CHAPTER 4 CONCLUSION	33
Bibliography	34
APPENDIX A Running Config of Router	36
POSTER	41
TURNITIN PLAGARISM CHECK RESULT	42

List of Tables

Table 1 Attack Effect Without NAT Load Balancing for Different values of sockets	
-----	26
Table 2 Attack Effect with Load Balancing Table 1 Without NAT Load Balancing for Different values of sockets	
-----	26

List of Figures

Figure 1 Waterfall methodology.....	20
Figure 2 Network Setup for Project Part One	22
Figure 3 IP Address Configurations of the Router	22
Figure 4 NAT Load Balancing Configurations CLI Commands	23
Figure 5 Devices Setup.....	24
Figure 6 Solaris Interface.....	26
Figure 7 Command used to launch attack with time interval of 1 seconds with 100 sockets.....	27
Figure 8 HTTP Header that Solaris send to the server	27
Figure 9 Error Message when legitimate trying to access site under DOS Attack	27
Figure 10 Legitimate User Should Able to see this page if the website able to load	28

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:
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

CHAPTER 1

1.0 Introduction

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).

- 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.

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 switch, 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.

Load balancing is not a new technology and it already existed quite some time ago, and there is special load balancing equipment that can be used to handle Distributed Denial of Service attack or handle large number of requests. NAT load balancing feature in the router also existed but so far it is not used as a method for Denial of Service mitigation.

NAT Load Balancing is the enhanced way of load balancing technique in which NAT Load Balancing is a more cost efficient way that can be used as a temporarily solution. So far NAT Load balancing is used for improve the WAN connectivity but not for Denial of service mitigation.

1.2 Project Scope

This project is a deployment and research project for DOS mitigation. Current devices which includes network equipment devices such as servers, switches and routers will be reconfigured as a new revamped network setup. Previous configurations will be cleared. New software or firmware might be installed on servers and network equipment respectively if necessary as the project progress.

1.3 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.

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.

1.4 Project Innovation and Contribution

1. Administration and deployment is not too complex and able to complete within certain time frame by only a single person

As long as the correct CLI command is issued in the router, the effect will take place as soon as instantly. By issuing the “show ip nat translations” command, an admin or the person in charge can see the which servers or device the packets are forwarded to.

2. No advance coding or script writing skills is required.
3. This is a low cost mitigation technique for DOS or small scale DOS compared to others.

A particular organization can use their current servers, workstations and desktop computers to act as servers that can provide the service.

4. Only routers, multiple servers and multiple NICs are used instead of Load Balancer or any other extra security devices.

1.5 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 used 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.

CHAPTER 2 LITERATURE REVIEW

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 have other advance features besides blocking, dropping packets and logging. They are capable of sensing and stopping possible attacks. (IPS and IDS, 2011)

IDS systems only detects intrusion, log the attack and send alerts to administrator. IDS systems does 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 is 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 is the traffic legit and normal. (IPS and IDS, 2011)

Despite IDS and IPS have the ability to sense the attack but there are several issue 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 be 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 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

it 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. The entire traffic of a VLAN or network segment is replicated for sniffing. That traffic is then replicated by traditional switch hardware to serve it into the IDS/IPS system. In comparison, hypervisor and general OS routines are used by SDN to replicate the traffic. Experiments also have proven that SDN loses approximately 25% to 30% of attack vector events.

Besides faults in SDN software will cause problems in keeping track of 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, organization 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 from 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 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 address 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 requires 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.

CHAPTER 3 PROPOSED METHOD AND APPROACHES

3.0 Methods/ Technologies Involved

The methodology used for this project is using waterfall model because it is the most suitable methodology that suits this system implementation. The main reason is this implementation need to be divided into different phases. The next phase will only be carried out upon the completion of previous one. The planning and time schedules, target dates are the crucial part of this system deployment.

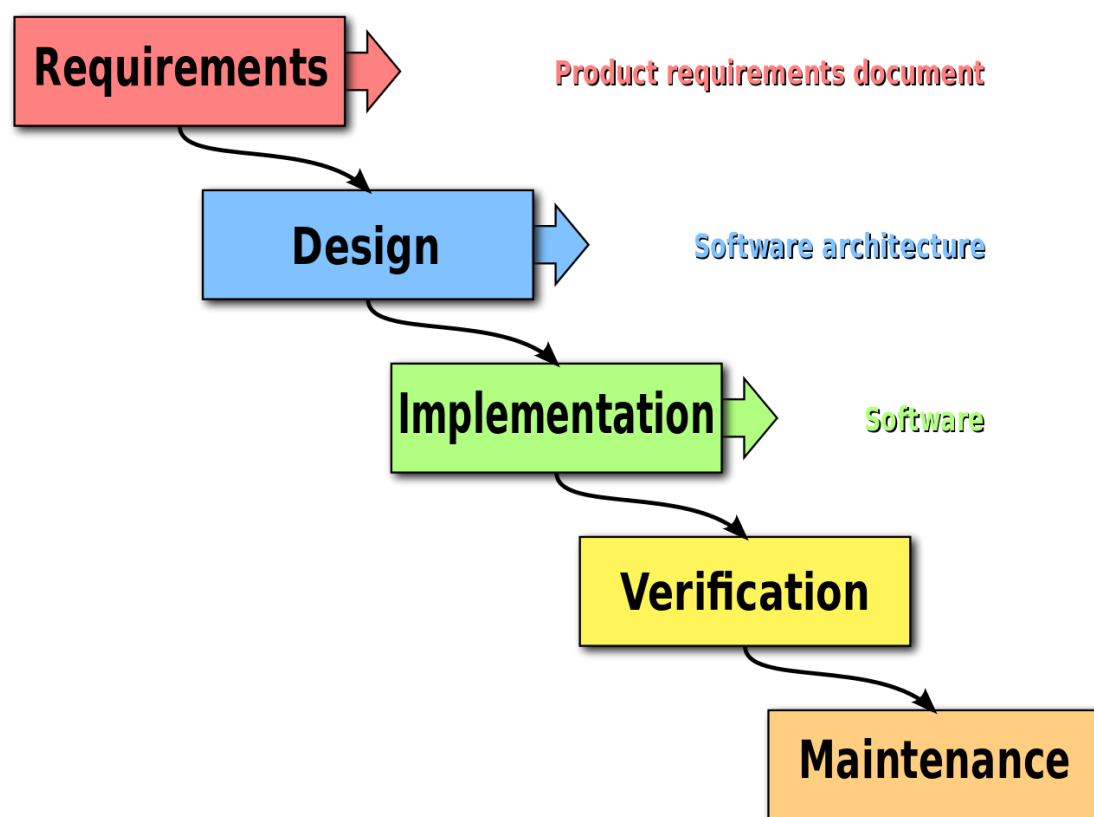


Figure 1 Waterfall methodology.

The progress flow of waterfall model in this project is

- Requirements: To get the requirements and set objectives
- Design: Drafting out the network setup as shown in Figure 1 and 4.
- Implementation: Deploying the equipment and configure them.
- Verification: Verify the accuracy of the deployment and correct any errors made

- e. Maintenance: Improve and revise the settings from time to time.

NAT will be use to fulfill the concept of load balancing. TCP Load Distribution configurations will be setup in a router to forward packets or request to all the devices with the same port number but different IP addresses for the same service in a rotary basis. Every new connection established will be forwarded to the next IP that is assigned in the pool.

This deployment or implementation is tested by launching the attack during the lowest possible strength at the configuration without TCP Load Distribution (Normal Port Forwarding). The strength is increase incrementally until the website show error message like “Connection Refused” on the legitimate user browser.

3.0.1 Tools / Software Used

1. WAMP Server with Apache 2.4.23
2. Kali Linux 2016.2 Version and Slowloris for making DOS Attack.
3. Cisco 1841 routers with firmware Version 12.4(25), R

3.0.2 Performance Definition

Website still able to load or respond during the attack.

3.1 System Design /Overview

. The network setup diagrams are shown in Figure 2 and 4.1.

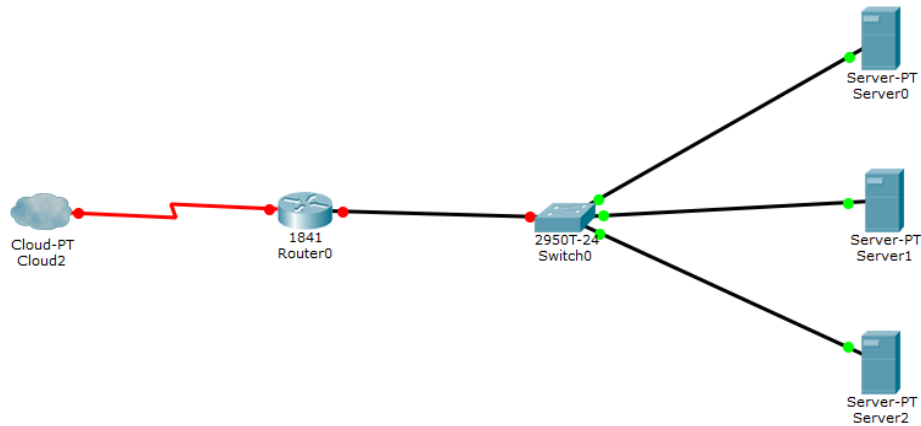


Figure 2 Network Setup for Project Part One

Figure 1 show part one of the network configuration of load balancing using single routers and multiple servers. Related commands for configurations are shown in Figure 2 and 3.

```
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 IP Address Configurations of the Router

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.

```
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 4 NAT Load Balancing Configurations CLI Commands

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 192.168.10.1 to 192.168.10.3 in round robin basis. 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.

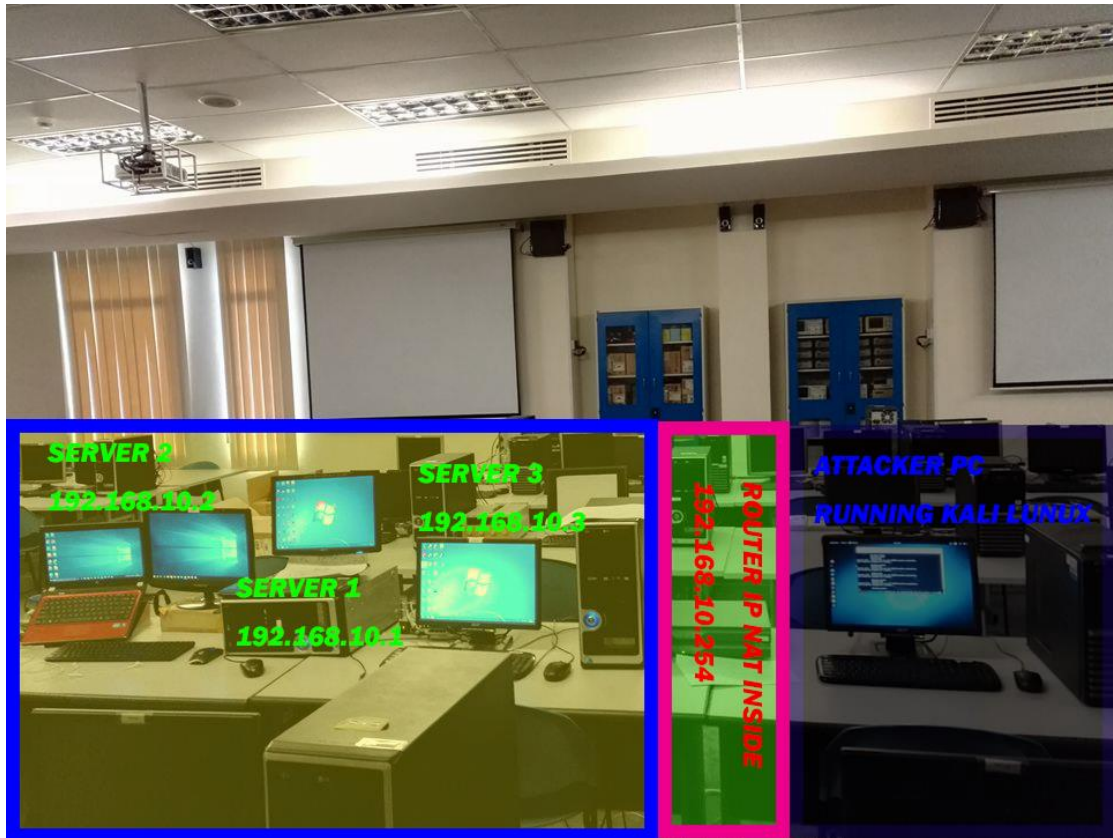


Figure 5 Devices Setup

Figure 4 illustrate the setup of the devices for this NAT Load Balancing deployment. The full running config of the router in Figure 1 is in the Appendix.

The second part of the project will use multiple WAN connections and multiple routers and multiple NICs. The number of routers used in this project is $N + 1$ where N is the number of WAN connections. Each of the N routers will do port forwarding to forward packets to the servers and one extra router which will do port forwarding to all the servers. This is illustrated in Figure 2.

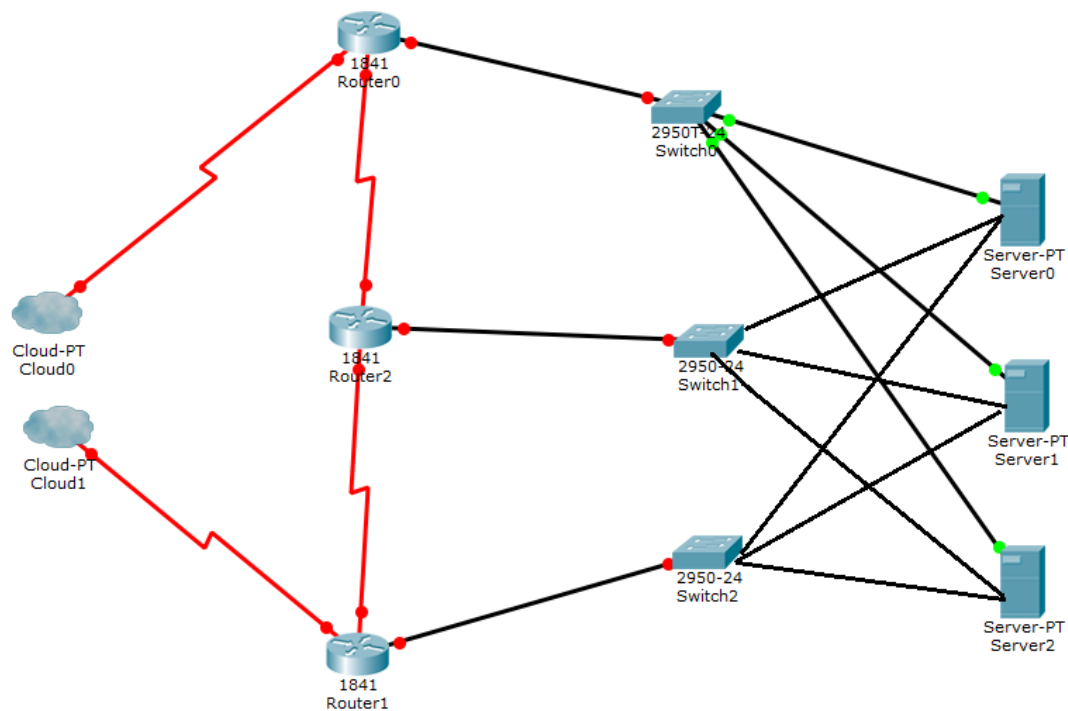


Figure 5.1 Network Setup for Project Part 2

The second part is to illustrate setup or deployment that can be done inside a particular organization after the ISP have done load balancing at the ISP side by diverting traffic to other connections going into the organization. This also to illustrate deployment that can be made to prevent SPOF.

Extra NIC cards will be installed in the servers. Static IPs will be configured in the routers and the servers.

3.2 Testing and Evaluation Descriptions with Results for First Part of Project

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.

Slowloris is using TCP State-Exhaustion attack but volumetric attack is possible if the server does not have enough resources to serve the connection requests.

Figure 6 Solaris Interface

The attack is first run on setup without NAT load Balancing with $t=1$ and $s=100$ with increment of 10 for s . 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. The command in Linux used to launch the

attack is shown in Figure 5

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

Figure 7 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 6. 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 8 HTTP Header that Solaris send to the server

As soon as the connection pool of the server 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 9.

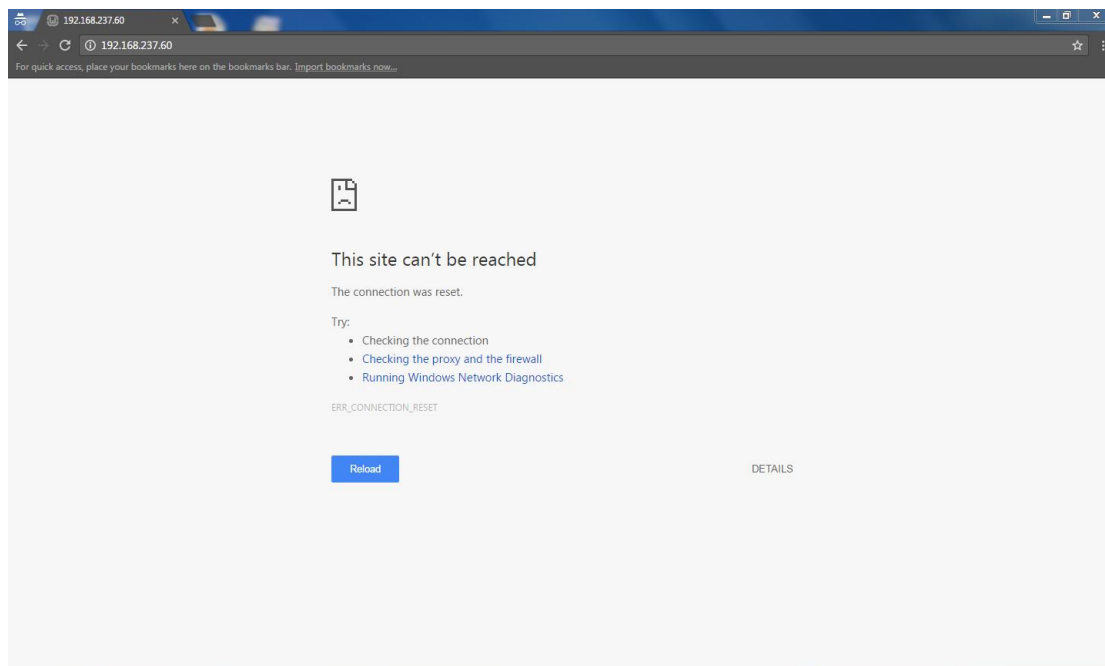


Figure 9 Error Message when legitimate trying to access site under DOS Attack

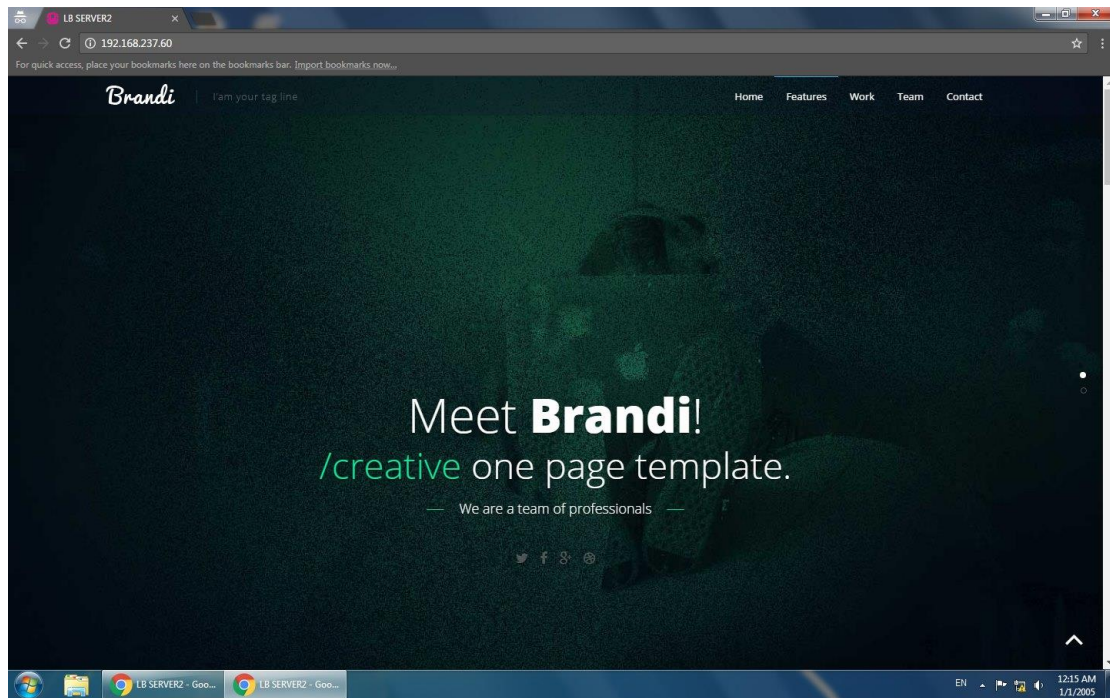


Figure 10 Legitimate User Should Able to see this page if the website able to load

However, with NAT Load Balancing implemented, legitimate user still able to access the website as illustrated in Figure 10 when the number of sockets per seconds is up to 800. At value of 900 and above, only Figure 9 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. The test results are for number of sockets versus whether is the website still accessible is illustrated in Table 1 and 2.

Number of Sockets Used	Is the Website Still Accessible ?
80	Yes
100	Yes
120	Yes
140	Yes
150	No

Table 2 Without NAT Load Balancing for Different values of sockets

Number of Sockets Used	Is the Website Still Accessible ?
150	Yes
300	Yes
450	Yes
600	Yes
750	Yes
900	No
1050	No
1200	No
1350	No

Table 2 Without NAT Load Balancing for Different values of sockets

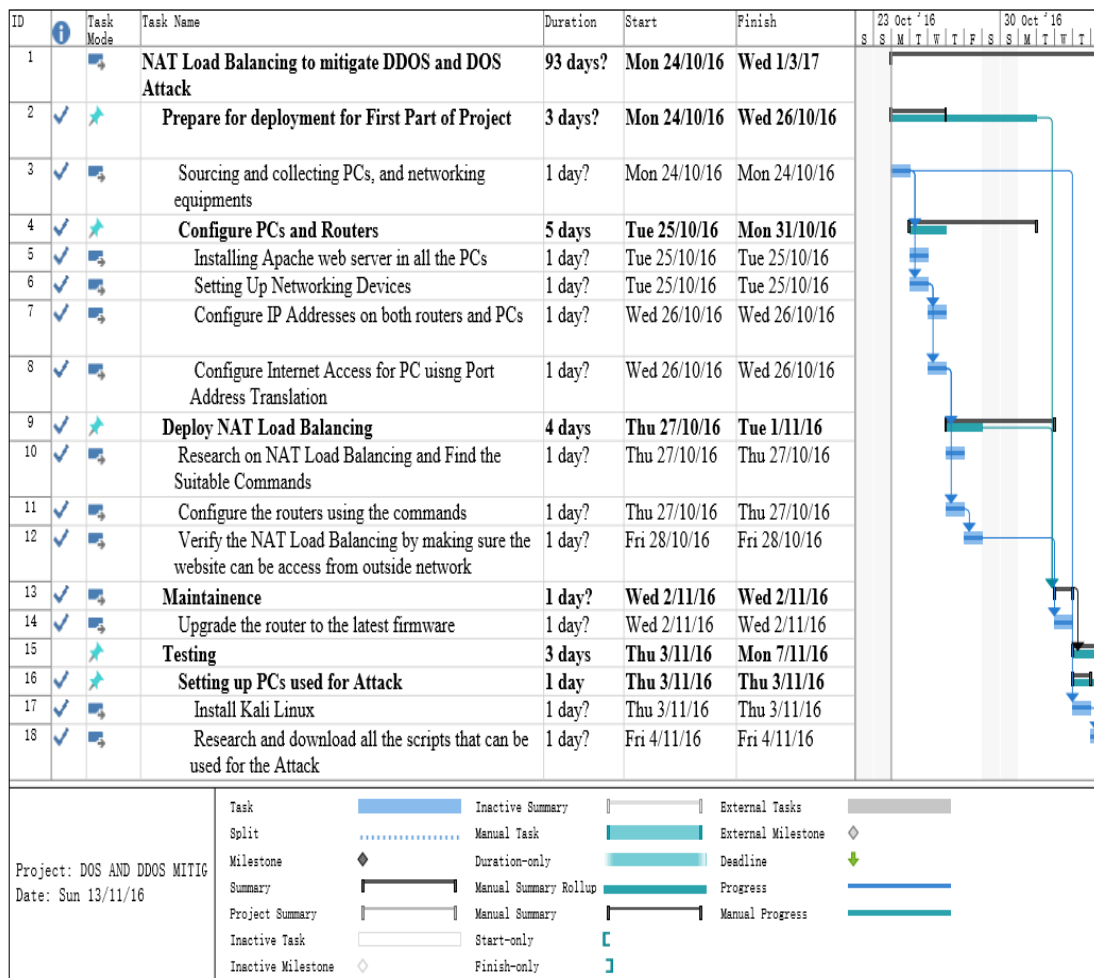
The NAT translation table during the attack is in the Appendix.

3.4 Implementation Issue and Challenges

1. Cisco 1841 router is considered as an old router and the firmware is out to date and doesn't support NAT Load Balancing. Research is needed to look for firmware for that router that support NAT Load Balancing. Precaution is needed not to "brick" the Router.
2. Choosing the attacking tools is a challenge. Tools like LOIC and HOIC actually brings no impact to the server even without load balancing and it requires a lot of system resources. Certain tools are compiled exe where there is no option to configure the intensity of the attack.

3.5 Timeline

This project is divided into two parts. The first part is just Load Balancing with one router and multiple servers and the second part more routers and other devices will be introduced. The first part of the project will be completed within this semester (October to December) whereas the second part will be completed latest by end of April next year.



ID	Task Mode	Task Name	Duration	Start	Finish	23 Oct '16	30 Oct '16
19		Perfrom First Test Without NAT Load Balancing	1 day	Mon 7/11/16	Mon 7/11/16	S	S
20		Backup the configurations for NAT Load Balancing	1 day?	Mon 7/11/16	Mon 7/11/16		
21		Configure Port Forwarding	1 day?	Tue 8/11/16	Tue 8/11/16		
22		Perform the attack with different Parameters finding the limit of the server	1 day?	Wed 9/11/16	Wed 9/11/16		
23		Perfrom Second Test With NAT Load Balancing	1 day	Tue 8/11/16	Tue 8/11/16		
24		Delete Port Forwarding and restore NAT Load Balancing configurations back	1 day?	Tue 8/11/16	Tue 8/11/16		
25		Perfrom the Attack With Different Parameter	1 day?	Wed 9/11/16	Wed 9/11/16		
26		Experiment Results Verification and Compilation	2 days	Thu 10/11/16	Fri 11/11/16		
27		Report Compilation	5 days	Mon 14/11/16	Fri 18/11/16		
28		Prepare for deployment for Second Part of Project	6 days?	Mon 16/1/17	Mon 23/1/17		
29		Sourcing and collecting PCs, and networking equipments	3 days	Mon 16/1/17	Wed 18/1/17		
30		Configure PCs and Routers	12 days	Thu 19/1/17	Fri 3/2/17		
31		Installing Extra NIC Cards on the PCs	1 day?	Thu 19/1/17	Thu 19/1/17		
32		Installing Apache web server in additional PCs if there is any	1 day?	Fri 20/1/17	Fri 20/1/17		
33		Setting up Extra Routers and Switches	2 days	Thu 19/1/17	Fri 20/1/17		

Project: DOS AND DDOS MITIG
Date: Sun 13/11/16

Task

Split

Milestone

Summary

Project Summary

Inactive Task

Inactive Milestone

Inactive Summary

Manual Task

Duration-only

Manual Summary Rollup

Manual Summary

Start-only

Finish-only

External Tasks

External Milestone

Deadline

Progress

Manual Progress

Page 2

ID	Task Mode	Task Name	Duration	Start	Finish	23 Oct '16	30 Oct '16
34		Configure IP Addresses on both routers and PCs	3 days	Mon 23/1/17	Wed 25/1/17	S	S
35		Configure VLAN and Additional Routes	5 days	Thu 26/1/17	Wed 1/2/17		
36		Deploy NAT Load Balancing For Single Point of Failure	4 days?	Thu 2/2/17	Tue 7/2/17		
37		Configure the routers using the commands	4 days	Thu 2/2/17	Tue 7/2/17		
38		Verify the NAT Load Balancing by making sure the website can be access from outside network	1 day?	Thu 2/2/17	Thu 2/2/17		
39		Maintainence	1 day?	Wed 8/2/17	Wed 8/2/17		
40		Upgrade the router to the latest firmware	1 day?	Wed 8/2/17	Wed 8/2/17		
41		Testing	15 days?	Thu 9/2/17	Wed 1/3/17		
42		Setting up PCs used for Attack	1 day?	Thu 9/2/17	Thu 9/2/17		
43		Install Kali Linux for additional PC that is /are introduced	1 day?	Thu 9/2/17	Thu 9/2/17		
44		Perfrom First Test Without Tweaking OS	3 days	Fri 10/2/17	Tue 14/2/17		
45		Perform the attack with different Parameters finding the limit of the server	1 day?	Fri 10/2/17	Fri 10/2/17		
46		Compare the results collected here with the results collected in the First Part	1 day?	Fri 10/2/17	Fri 10/2/17		
47		Perfrom Second Test With OS Tweaking (Optional)	6 days	Thu 9/2/17	Thu 16/2/17		
48		Modify settings and Config File of Apache Server	3 days	Thu 9/2/17	Mon 13/2/17		
49		Perfrom the Attack With Different Parameter	3 days	Tue 14/2/17	Thu 16/2/17		

Project: DOS AND DDOS MITIG
Date: Sun 13/11/16

Task

Split

Milestone

Summary

Project Summary

Inactive Task

Inactive Milestone

Inactive Summary

Manual Task

Duration-only

Manual Summary Rollup

Manual Summary

Start-only

Finish-only

External Tasks

External Milestone

Deadline

Progress

Manual Progress

Page 3

ID		Task Mode	Task Name	Duration	Start	Finish	23 Oct '16							30 Oct '16						
50			Experiment Results Verification and Compilation	3 days	Mon 13/2/17	Wed 15/2/17	S	S	M	T	W	T	F	S	S	M	T	W	T	F
51			Final Report Compilation	10 days	Thu 16/2/17	Wed 1/3/17														

CHAPTER 4 CONCLUSION

Denial of Service or Distributed Denial of Service attack is the common attack that will face by organizations or people that host their own websites or services. However, some Denial of Service have more impact but some are not. Deploying anti-DDOS devices is very costly and it does not guarantee its effectiveness. Future more, it is redundant and a waste of the resources. However, if nothing is deployed, legitimate users will not able to access the website during the attack. NAT Load Balancing is the cost-effective solution to mitigate Denial of Service or DDOS that is at a small scale by using TCP Load Distribution. Tests also have verified that NAT Load Balancing is able to mitigate the attack. Users can still access the website for a longer period even if the scale is slightly larger. NAT Load Balancing is also easy to implement because it can be done at the router side. Additional routers and routes can also be introduced to prevent Single Point of Failure. 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.

Bibliography

1. ARBOR Networks, 2013. *DDoS Mitigation Best Practices*. [Online]
Available at:
[https://www.arbornetworks.com/images/documents/Arbor%20Insights/AI_DDoS Mitigation_EN2013.pdf](https://www.arbornetworks.com/images/documents/Arbor%20Insights/AI_DDoS_Mitigation_EN2013.pdf)
[Accessed 11 August 2016].
2. B. B. Gupta, S. M. I. R. C. J. a. M. M. M. I., 2010. Distributed Denial of Service Prevention Technique. *International Journal of Computer and Electrical Engineering*, 2(2), pp. 268-276.
3. Davis, B., 2010. Leveraging the Load Balancer to Fight DDoS. *SANS Institute InfoSec Reading Room*.
4. F5 Networks Inc, n.d. *Glossary and Terms : Load Balancer*. [Online]
Available at: <https://f5.com/glossary/load-balancer>
[Accessed 10 August 2016].
5. Gates, S., 2013. *DDoS ATTACKS: MOTIVES, MECHANISMS AND MITIGATION*. s.l., s.n.
6. Geer, D., n.d. *Five reasons IT pros are not ready for SDN investment*. [Online]
Available at: <http://searchsdn.techtarget.com/feature/Five-reasons-IT-pros-are-not-ready-for-SDN-investment>
[Accessed 10 August 2016].
7. HAProxy, 2012. *USE A LOAD-BALANCER AS A FIRST ROW OF DEFENSE AGAINST DDOS*. [Online]
Available at: <http://blog.haproxy.com/2012/02/27/use-a-load-balancer-as-a-first-row-of-defense-against-ddos/>
[Accessed 10 August 2016].
8. Internet-Computer-Security.com, n.d. *IPS (Intrusion Prevention System) and IDS (Intrusion Detection Systems)*. [Online]

Available at: <http://www.internet-computer-security.com/Firewall/IPS.html>

[Accessed 9 August 2016].

9. Kenig, R., 2013. *Can your firewall and IPS block DDOS Attacks ?*. [Online]
Available at: <https://blog.radware.com/security/2013/05/can-firewall-and-ips-block-ddos-attacks/>
[Accessed 10 August 2016].
10. Kiggins, A. & Lyon, J., 2016. *AWS Best Practices for DDoS Resiliency*, s.l.: Amazon Web Services.
11. MATTHEWS, T., 2014. *Incapsula Survey: What DDOS Attacks really cost Business*, s.l.: Incapsula.
12. Nayana Y, M. G., 2015. DDoS Mitigation using Software Defined Network. *International Journal of Engineering Trends and Technology*, 24(5), pp. 258-264.
13. Palo Alto Networks, Inc, 2014. *Application DDoS Mitigation*, s.l.: Palo Alto Networks.
14. Radware, Ltd, 2013. *Approaches to Mitigate DDoS Attacks Whitepaper*, s.l.: Radware.
15. Turnbull, M., n.d. *Simple Denial Of Service DOS Attack Mitigation Using HAProxy*. [Online]
Available at: <http://loadbalancer.org/blog/simple-denial-of-service-dos-attack-mitigation-using-haproxy-2>
[Accessed 8 August 2016].
16. Villanueva, J. C., 2015. *Comparing Load Balancing Algorithms*. [Online]
Available at: <http://www.jscape.com/blog/load-balancing-algorithms>
[Accessed 10 August 2016].
17. *Slowloris* (no date) Available at: <https://www.incapsula.com/ddos/attack-glossary/slowloris.html> (Accessed: 14 November 2016).

APPENDIX A Running Config of Router

User Access Verification

Password:

Password:

ZJ>en

Password:

ZJ#show run

Building configuration...

Current configuration : 4398 bytes

!

version 12.4

service config

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname ZJ

!

boot-start-marker

boot-end-marker

!

no logging buffered

enable secret 5 \$1\$Helh\$yJ9HU68nxf1i0xDE1Gv07.

enable password csc

!

no aaa new-model

ip cef

!

!

no ip dhcp use vrf connected

!

ip dhcp pool DHCP2

network 192.168.10.0 255.255.255.0

dns-server 192.168.201.1

default-router 192.168.10.254 192.168.237.254 192.168.201.1

!

ip dhcp pool DCP2

!

```

!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
crypto pki trustpoint TP-self-signed-1637500100
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-1637500100
  revocation-check none
  rsakeypair TP-self-signed-1637500100
!
!
crypto pki certificate chain TP-self-signed-1637500100
  certificate self-signed 03
    3082023A 308201A3 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
    31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
    69666963 6174652D 31363337 35303031 3030301E 170D3730 30313133 30323132
    33385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
    4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 36333735
    30303130 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
    8100AB32 D5193A49 471EB368 FBF479EF 7D08102E 722C8046 45F9151A F40B4F01
    932D1427 D1841A2E 418DC46C 9560A9C1 BCE997C8 152E7D0A 30B65B2C B306618F
    2412A90D 56BB4CA3 7D70CBB7 360A9619 845F247C 144270A0 5F9F176C 6CB73C85
    9B3B5B48 21E02C11 D4DA1722 AE185667 9EF1F9B6 84CCC9CF B0838806 9A34EEB9
    A67F0203 010001A3 62306030 0F060355 1D130101 FF040530 030101FF 300D0603
    551D1104 06300482 025A4A30 1F060355 1D230418 30168014 1CEE557F D5BBA85F
    153D6084 41E8CAC3 2D70AE11 301D0603 551D0E04 1604141C EE557FD5 BBA85F15
    3D608441 E8CAC32D 70AE1130 0D06092A 864886F7 0D010104 05000381 810094A6
    1E97E7C8 53E0AA16 C9743E0F 0711C10C 3A169006 54CA16F6 4CE97245 C8F43241
    A53421FD 0EA6F51E E3820B1A F1DFA246 20DA6DB7 C3FE35E9 F50F1003 F1C7C3E0
    77A8954A 4B7980B7 0A542020 C4378590 FF79FA5B B60EC3C4 5529CA92 259DB1A2
    5EB96611 AA5527B4 DF2C6368 0169A9DC CFF02626 0C8C092C 78C1A9E8 F69A
  quit
!
!
!
class-map match-any SDM-Transactional-1
  match dscp af21
  match dscp af22
  match dscp af23
class-map match-any SDM-Signaling-1
  match dscp cs3

```

```

    match dscp af31
class-map match-any SDM-Routing-1
    match dscp cs6
class-map match-any SDM-Voice-1
    match dscp ef
class-map match-any SDM-Management-1
    match dscp cs2
!
!
policy-map SDM-QoS-Policy-1
    class SDM-Voice-1
        priority percent 33
    class SDM-Signaling-1
        bandwidth percent 5
    class SDM-Routing-1
        bandwidth percent 5
    class SDM-Management-1
        bandwidth percent 5
    class SDM-Transactional-1
        bandwidth percent 5
    class class-default
        fair-queue
        random-detect
!
!
!
!
!
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
!
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
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
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
```



POSTER

PROBLEM ?




 **Deploying Anti-DDOS Devices is costly. Not everyone has budget**



 **Not enough man power for administration and maintainence**

  **Redundant to implement expensive anti-DDDOS devies for some cases**





OBJECTIVES NAT LOAD BALANCING







TCP LOAD DISTRIBUTION
ROUND ROBIN

- 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 expend 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 performance of the server by tweaking the OS or related software.

WHY USE NAT LOAD BALANCING?



1. SIMPLE ADMINISTRATION AND DEPLOYMENT
2. NO ADBANCE CODING EXPEREINCE REQUIRED
3. LOW COST
4. REDUCE E-WASTE: ENCOURAGE THE USE OF OLD PC



BY LEE ZHI JIANG
SUPERVISOR: DR GAN MING LEE



TURNITIN PLAGARISM CHECK RESULT

Turnitin Document Viewer - Google Chrome

https://www.turnitin.com/dv?i=18007369267578u=1058145422&student_user=1&lang=en_us8

FYP1 Turnitin Oct2016 FYP1 Turnitin Oct2016 - DUE 31-Jan-2017

Originality GradeMark PeerMark

DENIAL OF SERVICE ATTACK MITIGATION USING NAT LOAD BALANCING

BY ZHI JIANG LEE

turnitin 8% SIMILAR OUT OF 9

Match Overview

1	searchsdn.techtarget.c...	Internet source	2%
2	B. B. Gupta, "Defendin...	Publication	2%
3	www.secdist.se	Internet source	1%
4	Submitted to Webster ...	Student paper	1%
5	Submitted to Middlese...	Student paper	<1%
6	www.ddosattacks.net	Internet source	<1%
7	Submitted to Kerala ...	Student paper	<1%
8	www.dji.com	Internet source	<1%
9	Submitted to Sabanci ...	Student paper	<1%
10	Submitted to Universit...	Student paper	<1%
11	www.stop-hackers.org	Internet source	<1%
12	Submitted to Rocheste...	Student paper	<1%

CHAPTER 1

1.0 Introduction

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 intension 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).

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., 2013).

PAGE: 1 OF 25

Text-Only Report

FINAL YEAR PROJECT WEEKLY REPORT

(Project I / Project II)

Trimester, Year: Y3 T2	Study week no.: 1
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

Day 1

Setting up and deploying equipment in the laboratory which includes, routers, switches, power supplies and PCs.

Configure the PCs to act as web servers by installing Apache web server on port 80 by using WAMP Server.

The initial routers and switch used are wireless router D-Link dir-615 and a mini 5 port switch. The router and switch are just to test the basic network connectivity and port forwarding.

Day 2 - 3

The home router and switch is then replaced with industrial standard router Cisco 1841 and Cisco 1200 series, 8 port switch. The routers are configured with basic configurations which includes IP Address on the interfaces. No routing or NAT were configured yet.

Day 4 -5

Setting up basic NAT configurations which includes Port forwarding. One interface is reconfigured to DHCP client which will obtain IP Address from the DHCP Server in the lab. This interface is configured as WAN port. The other interface is connected to the switch. DHCP pool is configured here to allocate IP Address for the servers. IP Routing is enabled. Test is done using one of the PC in the lab to access the ip address obtained in the interface connected to the WAN interface.

2. WORK TO BE DONE

- Research on DOOS attack methods
- Research on NAT Load Balancing Implementations
- Configure NAT Load Balancing on the router
- Tidying up the running-config such as remove configurations that no longer needed.
- Tidying up the wiring to make the work space neater with necessary labeling.

3. PROBLEMS ENCOUNTERED

- Not able to connect to the router CLI config using serial connection at the first try. Able to fix it by changing another serial port.

The router is in recovery mode.

4. SELF EVALUATION OF THE PROGRESS

There is more room for improvement in terms of the speed of setting up the equipment.

Supervisor's signature

Student's signature

Trimester, Year: Y3 T2	Study week no.: 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

1. Download Executable DOS tool
2. Configure Port Forwarding and Backup the configuration
3. Configure NAT Load Balancing and backup the configuration
4. Upgrade router firmware

2. WORK TO BE DONE

- Research on more DOOS attack methods
- Tidy up workspace

3. PROBLEMS ENCOUNTERED

4. SELF EVALUATION OF THE PROGRESS

Supervisor's signature

Student's signature

Trimester, Year: Y3 T2	Study week no.: 3
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

Testing by launching attack using executable DDOS tool. Observe the impact with and without Load Balancing.

2. WORK TO BE DONE

- Research on DOOS attack methods
- Fine tune the system.

3. PROBLEMS ENCOUNTERED

Unable to modify the parameter. The attack is too massive where the servers cannot handle it.

4. SELF EVALUATION OF THE PROGRESS

Supervisor's signature

Student's signature

Trimester, Year: Y3 T2	Study week no.: 4
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

1. Download and Install Kali Linux on hard disk using Dual Boot
2. Download Slowloris Perl script
3. Repeat DOS attack and obtain result for both with and without NAT Load Balancing
4. Finalize result and Report compilation.

2. WORK TO BE DONE

Tidy up workspace

3. PROBLEMS ENCOUNTERED

4. SELF EVALUATION OF THE PROGRESS

Supervisor's signature

Student's signature

THIS PAGE IS INTENTIONALLY LEFT EMPTY