SMALL SCALE DISTRIBUTED DENAIL OF SERVICE AND 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)

MAY 2016

Table of Contents

List of Tables

List of Figures

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

CHAPTER 1 PROJECT BACKGROUND

1.0 Introduction

DDOS Attack is an issue of concern in the Internet World which includes organization because this attack always increases by time. RSA Conference Asia Pacific 2013 highlighted that according to Akamai's "State of Internet" report for the fourth quarter of 2012, the amount of DDOS attacks had 200% increment compared to 2011. The awareness about the consequences of the threat to online services offered increases. 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). RSA Conference Asia Pacific 2013 explained the history of DDOS Attacks and Attackers with hackers hacking for fun purpose as the beginning followed by cyber criminals for profit, cyber armies' politics, cyber terrorist to cause fear and last but not least cyber hacktivist for certain agenda. DDOS attacks are used by governments or activist groups to assist in achieving political agendas as common tools. (Ristic, 2005).

1.0.1 DDOS Primer (Arbor Networks, 2013).

Many research papers, articles and posters by security conferences has their own way in giving definition of DOS but all of them are similar which is an attempt to prevent others from using the service using all kinds of ways and methods. This attempt is made by a solo user unlike DDOS which consists of multiple users simultaneously. Although there are still many solo DOS attackers but the majority of the attacks today are DDOS. 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.

1.0.2 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 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 shows the demonstration of attacks using those tools. (Gates, 2013)

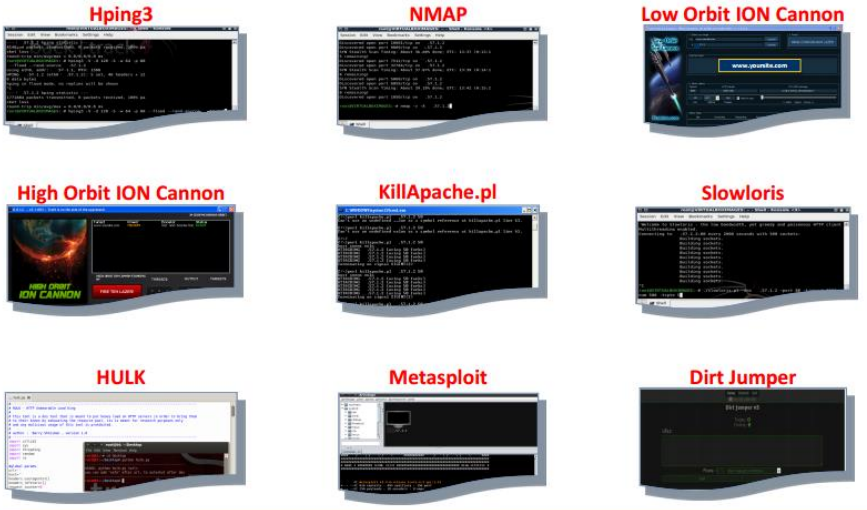

Figure 1 Sample tools used to perform DDOS Attack (Gates, 2013)

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.

1.1 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)

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.

1.2 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.

CHAPTER 2 LITERATURE REVIEW

To begin with, many organizations have their own way of DDOS prevention as well as DDOS mitigation. They are many anti DDOS services available offered by service provider. Besides that, they 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. There 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 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 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, 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 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 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 PROJECT SCOPE AND OBJECTIVES

3.0 Project Scope

Although DDOS is the topic mentioned in Chapter 1 and Chapter 2, but the scope in this chapter is narrowed down to a small scale DDOS attack or just simply DOS attack only. We have the assumption here whereby we have more than enough bandwidth but not system resources such as processing power and memory.

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.

3.1 Project Outline / Model

The concept of load balancing will be used in this project. However, instead of using load balancing devices, combinations of multiple devices and equipment with new configurations and setup will serve the purpose of load balancing. Current, old and refurbished devices is considered and will be used in this project.

3.2 Project Objectives

1. This project is aim to mitigate DDOS attack by using NAT load balancing.
2. Legitimate users are still able access the service with minimal degrade of service quality.
3. Single point of failure can be mitigated by using extra routers and routes.

3.3 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
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.
4. Only routers, multiple servers and multiple NICs are used instead of Load Balancer or any other extra devices.

CHAPTER 4

3.0 Methods/ Technologies Involved

NAT will be use to fulfill the concept of load balancing. Port forwarding 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. Round robin algorithm will be used to decide which device to forward the packets to. Least connection or weighted round robin will be use depending the specifications of the serer behind the router. This is the first part of the project. This is illustrated in

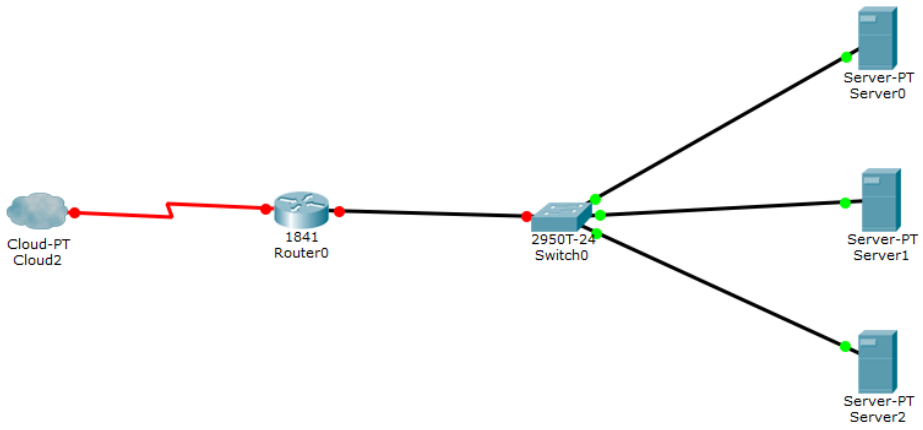

Figure 2 Network Setup for Project Part One

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

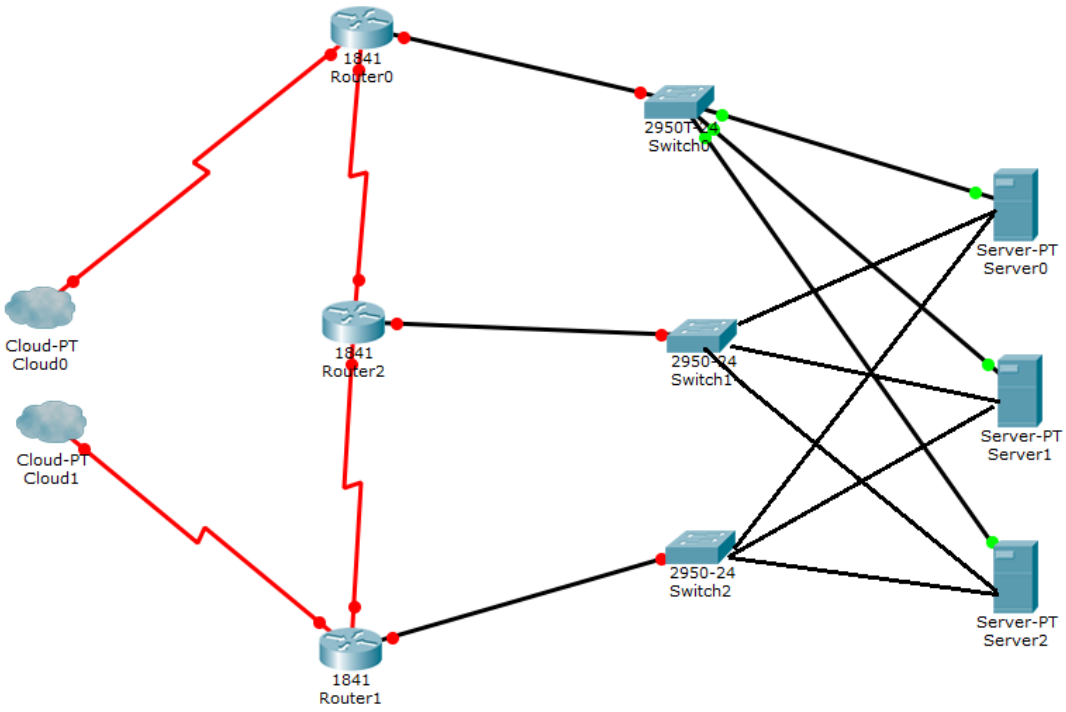

Figure 3 Network Setup for Project Part 2

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.

3.1 Testing and Evaluation Methods

Simulation software will be used to verify the flow of the packets from the routers to the devices to ensure this method is workable. The ideal result is we will be able to see packets traverse through different routes to multiple devices instead of by using one route to one device only.

In order to test this method in real life, web pages and databases with the same content will be hosted in all the PC using WAMP. The contents will be synchronizing between all the PCs. A medium complex website will be hosted which will involve database query process. Performance will be evaluated by using response time took to load the website and perform a certain operation which requires database query with different amount of attack bandwidth. The bandwidth used as response time will be recorded in a table as shown in Table 1.

3.1.1 First attack (Only one router and one host)

Several types of attack tools and bots will be running simultaneously against the host with incremental amount of bandwidth. They will be 1 host involved in the attack to simulate DOS attack followed by 3 hosts to simulate DDOS attack. A timer is then started. Another PC will be simulating a legitimate user trying to access the page and perform certain activity that involved database query which includes searching for an item existed in the database, log in and register. The response time will be recorded against the bandwidth.

This process will be performing repeatedly until the host no longer respond to legitimate user requests. The time taken for the host to stop responding is taken and recorded as t_b

3.1.2 Second Attack (Network setup as in Figure 2)

The same steps in 3.1.1 are repeated and the time will be recorded as t_{ai}, where t_{ai} is the time taken until legitimate user unable to access to the host.

The objective is achieved if the response time is lower compared to the first attack. The target IP Address of this attack will be the public IP Address which is the IP Address of the WAN interface.

3.1.3 Third Attack (On network setup in Figure 3)

The same steps in 3.1.1 and 3.1.2 are repeated. Response time is expected to be lower than the response time collected in 3.1.1 and 3.1.2.

3.1.4 Variables Definition

Constant Variable: Number of hosts involved in DDOS Attack

Manipulated Variable: Bandwidth Used

Responding Variable: Response Time for the host to process the request by legitimate user.

Bandwidth Used (mbps)	Response Time (ms)
5	
10	
15	
20	
25	
30	
35	
40	
45	
50	
55	
60	
65	
70	
75	
80	
85	
90	

Table 1 Bandwidth Used Versus Response Time tabulation format

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
   [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 Auguest 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 HAProx.* [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].