

**INFORMATION SEARCH and ANALYSIS SKILLS**

**ISAS**

**“Mitigation Techniques Web Application Firewall On DDoS"**

Arranged by:

1. Kapten Bintang
2. M.Dani Setiawan

Faculty:

Fachran Nazarullah S.Kom

**CONTINUING EDUCATION PROGRAM CENTER FOR COMPUTING AND INFORMATION TECHNOLOGY**

**FACULTY OF ENGINEERING, UNIVERSITY OF INDONESIA**

**2020**

**PREFACE**

Praise God Almighty, for the presence of plenty of mercy and his grace, so that we can complete this Information Search and Analysis Skills (ISAS) with the title “Mitigation Techniques Web Application Firewall on DDoS”. Without His mercy, we would not be able to complete this project in time. Even though there are many obstacles that author face on making this project, but finally author can finish this project.

The author also thanked Mr. Fachran Nazarullah as a lecturer who has provided guidance to the author and advice in the process of preparing this ISAS. Not to forget the author thanked the various parties who have provided encouragement and motivation so that the ISAS can be completed on time

Author know that the results of this article is far from perfect and there are still many shortcomings, author hope readers will give comments and suggestions in building this article in order to become better. We hope this article can be useful for those who read or hear, especially for CCIT students of the Faculty of Engineering UI.

Thank you,

Depok,3 March 2020

Author

**TABLE OF CONTENTS**

**PREFACE i**

**TABLE OF CONTENTS ii**

**TABLE OF FIGURE iii**

**CHAPTER I INTRODUCTION 1**

1. Background 1
2. Writing Objective 2
3. Problem Domain 2
4. Writing Methodology 3
5. Writing Framework 3

**CHAPTER II BASIC THEORY 4**

1. Explanation of Cyber Security 4
2. Explanation of Web Threat 4
3. Types of Attacks on Computer Networks 5
4. Explanation of DDoS 8
5. Explanation of Web Application Firewall 8

**CHAPTER III PROBLEM ANALYSIS**

1. How Does DDoS Attack Works 9
2. How DDoS Mitigation Works 14
3. An Architecture for Web Application Firewall 15

**CHAPTER IV CONCLUSION & SUGGESTION 18**

4.1 Conclusion 18  
4.2 Suggestion 18

**BIBILIOGRAPHY 19**

**TABLE OF FIGURES**

Figure 3.1 How DDOS Attacks Work 9

Figure 3.2 Common Types of DDOS Attack 10

Figure 3.3 Application Layer Attacks 11

Figure 3.4 SYN Flood 12

Figure 3.5 DNS Amplification 13

Figure 3.6 Web Application Firewall 15

Figure 3.7 Architecture WAF 16

Figure 3.8 DDOS Mitigation 17

**CHAPTER I  
INTRODUCTION**

1. **Background**

Security is a condition where humans or objects, avoided from the danger taken or disturbed, then will cause a feeling of calm and comfort. Security can be obtained through several ways, one of them using and published technology. The application of security technology is now highly developed, fast, starting from conventional methods to high-tech.

The internet has become a trend for many people to find information, communicate, and socialize.Various information such as news, entertainment, and personal information etc. are displayed on the website. It is undeniable that the internet not only provides many benefits, but creates new crimes committed through computer media. Crimes in the world of technology and information specifically on web applications more often. Many members appeared intentionally getting confidential information from a website.

At this time the number of outside attacks launched by attackers is more varied and varied. Examples are ddos (Distributed Denial of Service), bruteforce and Scanning attacks. DDOS attacks cause the system being attacked to experience interference in the form of error requests, halt, system failure and so on. Any system that provides TCP-based network services has the potential to be hit by a DDOS syn flood attack.

DDoS attacks began to be intensified since the late 2000s, and since then the size of attacks has continued to increase significantly in recent years. The protocol exploitation and amplification of the new attack became too large for most companies to deal with it without the support of cloud-based DDoS scrubbing services. In 2013, it was reported that the SpamHaus service was "successfully" disabled by a 300 Gbps attack. Meanwhile, in 2014 there was an attack with a fantastic number of 400 Gbps.

However, the biggest DDoS attack in the world occurred in 2015 with attacks of up to 500 Gbps. With bandwidth costs becoming increasingly affordable,

it is now easier to launch attacks with sizes that can reach terabytes in the future.

1. **Writing Objective**
2. Explanation of Cyber Security
3. Explanation of Web Threat
4. Types of Attacks on Computer Networks
5. Explanation of DDoS
6. Explanation of Web Application Firewall
7. **Problem Domain**

Accordance with the title of ISAS "Mitigation Techniques to Stop DDoS Attacks" We will discuss:

1. How Does DDoS Attacks
2. How DDoS Mitigation Works
3. An Architecture for Web Application Firewall
4. **Writing Methodology**

**Library Research Method**

Collecting data with browsing information from reference source contain on online sites that relate with the topic of this ISAS.

**Discussion Method**

After collecting data from reference source, we discuss and compose the data into structure contents for completing this ISAS.

1. **Writing Framework**
   * 1. **Chapter I Introduction**

* Background
* Writing Objectives
* Problem Domain
* Methodology
* Writing Framework
  + 1. **Chapter II Basic Theory**
* Explanation of Internet Security
* Explanation of Web Threat
* Types of Attacks on Computer Networks
* Explanation of DDoS
* Explanation of Web Application Firewall
  + 1. **Chapter III Problem Analysis**
* How Does DDoS Works
* How DDoS Mitigation Works
* An Architecture for Mitigating DDoS Attacks
  + 1. **Chapter IV Conclusion**
* Conclusion
* Suggestion

**CHAPTER II**

**BASIC THEORY**

1. **Definition Cyber Security**

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security comprises cybersecurity and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems. The goal of cybersecurity is to limit risk and protect IT assets from attackers with malicious intent. Information security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cybersecurity.

Cybersecurity best practices can, and should, be implemented by large and small organizations, employees and individuals. One of the most problematic elements of cybersecurity is the continually evolving nature of security risks and advanced persistent threats (APTs).

The traditional approach has been to focus resources on crucial system components and protect against the biggest known threats, which meant leaving components undefended and not protecting systems against less dangerous risks. To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach.

The National Institute of Standards and Technology (NIST), for example, recently issued updated guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments. Version 1.1 of the Framework for Improving Critical Infrastructure was released in April 2018. The voluntary Cybersecurity Framework (CSF), developed for use in the banking, communications, defense and energy industries, can be adopted by all sectors, including federal and state governments. President Donald Trump issued an executive order mandating that federal agencies adopt the NIST CSF in May 2017.

1. **Explanation of Web Threat**

Web-based threats – or online threats – are malware programs that can target you when you’re using the Internet. These browser-based threats include a range of malicious software programs that are designed to infect victims’ computer

A threat is any circumstance or event with the potential to adversely impact data or systems via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. Threats may involve intentional actors (e.g., attacker who wants to access information on a server) or unintentional actors (e.g., administrator who forgets to disable user accounts of a former employee.) Threats can be local, such as a disgruntled employee, or remote, such as an attacker in another geographical area.

Network traffic typically passes through intermediate computers, such as routers, or is carried over unsecured networks, such as wireless hotspots. Because of this, it can be intercepted by a third party. Threats against network traffic include the following; DDOS Network attack. The volume and strength of DDoS attacks are growing as hackers try to bring organizations offline or steal their data by flooding websites and networks with spurious traffic.

**2.3 Types of Attack of Computer Network**

Many people rely on the Internet for many of their professional, social and personal activities. But there are also people who attempt to damage our Internet-connected computers, violate our privacy and render inoperable the Internet services.

Given the frequency and variety of existing attacks as well as the threat of new and more destructive future attacks, network security has become a central topic in the field of computer networking.

1. **Malware** – short for malicious software which is specifically designed to disrupt, damage, or gain authorized access to a computer system. Much of the malware out there today is self-replicating: once it infects one host, from that host it seeks entry into other hosts over the Internet, and from the newly infected hosts, it seeks entry into yet more hosts. In this manner, self-replicating malware can spread exponentially fast.
2. **Virus** – A malware which requires some form of user’s interaction to infect the user’s device. The classic example is an e-mail attachment containing malicious executable code. If a user receives and opens such an attachment, the user inadvertently runs the malware on the device.
3. **Worm** – A malware which can enter a device without any explicit user interaction. For example, a user may be running a vulnerable network application to which an attacker can send malware. In some cases, without any user intervention, the application may accept the malware from the Internet and run it, creating a worm.
4. **Botnet** – A network of private computers infected with malicious software and controlled as a group without the owners’ knowledge, e.g. to send spam.
5. **DoS** (Denial of Service) – A DoS attack renders a network, host, or other pieces of infrastructure unusable by legitimate users. Most Internet DoS attacks fall into one of three categories :

• Vulnerability attack: This involves sending a few well-crafted messages to a vulnerable application or operating system running on a targeted host. If the right sequence of packets is sent to a vulnerable application or operating system, the service can stop or, worse, the host can crash.

• Bandwidth flooding: The attacker sends a deluge of packets to the targeted host—so many packets that the target’s access link becomes clogged, preventing legitimate packets from reaching the server.

• Connection flooding: The attacker establishes a large number of half-open or fully open TCP connections at the target host. The host can become so bogged down with these bogus connections that it stops accepting legitimate connections.

1. **DDoS** (Distributed DoS) – DDoS is a type of DOS attack where multiple compromised systems, are used to target a single system causing a Denial of Service (DoS) attack. DDoS attacks leveraging botnets with thousands of comprised hosts are a common occurrence today. DDoS attacks are much harder to detect and defend against than a DoS attack from a single host.
2. **Packet sniffer** – A passive receiver that records a copy of every packet that flies by is called a packet sniffer. By placing a passive receiver in the vicinity of the wireless transmitter, that receiver can obtain a copy of every packet that is transmitted! These packets can contain all kinds of sensitive information, including passwords, social security numbers, trade secrets, and private personal messages. some of the best defenses against packet sniffing involve cryptography.
3. **IP Spoofing** – The ability to inject packets into the Internet with a false source address is known as IP spoofing, and is but one of many ways in which one user can masquerade as another user. To solve this problem, we will need end-point authentication, that is, a mechanism that will allow us to determine with certainty if a message originates from where we think it does.
4. **Man-in-the-Middle** Attack – As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.
5. **Compromised-Key Attack** – A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack.
6. **Phishing** – The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
7. **DNS spoofing** – Also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver’s cache, causing the name server to return an incorrect IP address.

**2.4 Explanation About DDoS**

A distributed denial of service (DDoS) attack is when an attacker, or attackers, attempt to make it impossible for a service to be delivered. This can be achieved by thwarting access to virtually anything: servers, devices, services, networks, applications, and even specific transactions within applications. In a DoS attack, it’s one system that is sending the malicious data or requests; a DDoS attack comes from multiple systems.

Generally, these attacks work by drowning a system with requests for data. This could be sending a web server so many requests to serve a page that it crashes under the demand, or it could be a database being hit with a high volume of queries. The result is available internet bandwidth, CPU and RAM capacity becomes overwhelmed.

**2.5 Explanation About Web Application Firewall**

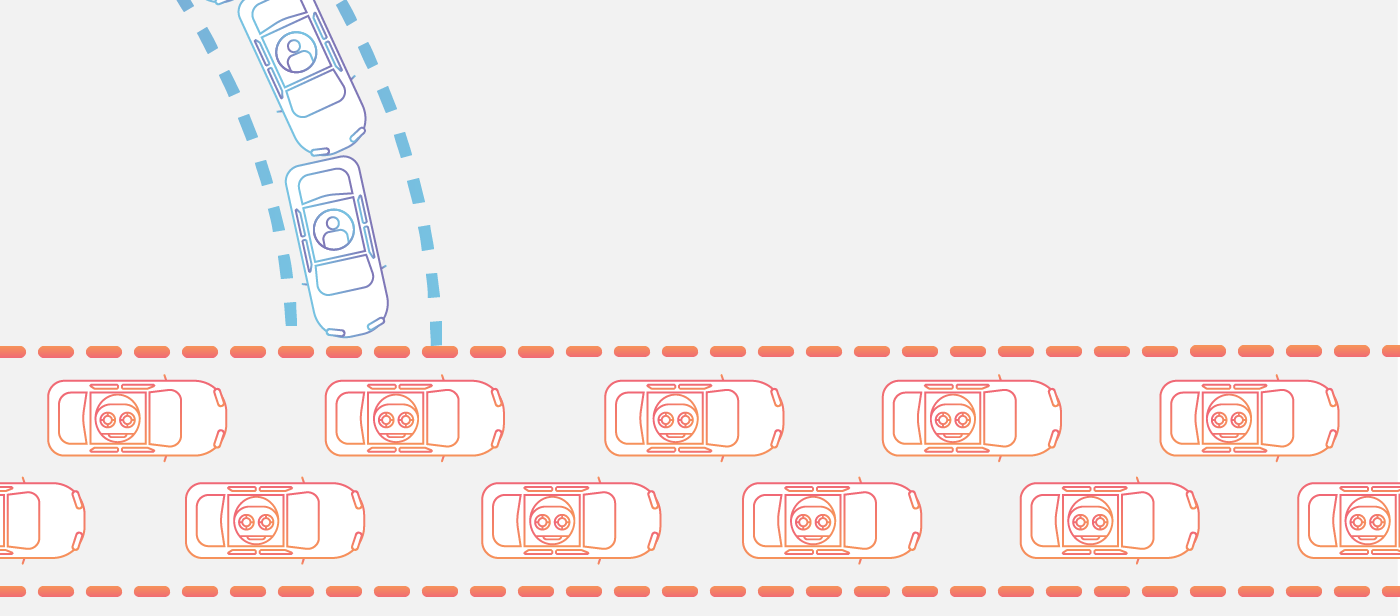
A web application firewall (WAF) is a firewall that monitors, filters and blocks data packets as they travel to and from a website or web application. A WAF can be either network-based, host-based or cloud-based and is often deployed through a reverse proxy and placed in front of one or more websites or applications. Running as a network appliance, server plugin or cloud service, the WAF inspects each packet and uses a rule base to analyze Layer 7 web application logic and filter out potentially harmful traffic that can facilitate web exploits.

Manual DDoS mitigation is no longer recommended because DDoS attackers can be avoided manually activated DDoS mitigation software. Other ways to prevent DDoS attacks can be done on-site and through a cloud-based solution provider. Through on-premise mitigation, technology (typically hardware devices) is placed in front of the network, with the risk that the filtering capacity is limited to the filtering device capacity. A middle option has a hybrid solution with on-site filtering support with cloud-based filtering.

**CHAPTER III**

**PROBLEM ANALYSIS**

**3.1 How Does DDoS Attack Work**



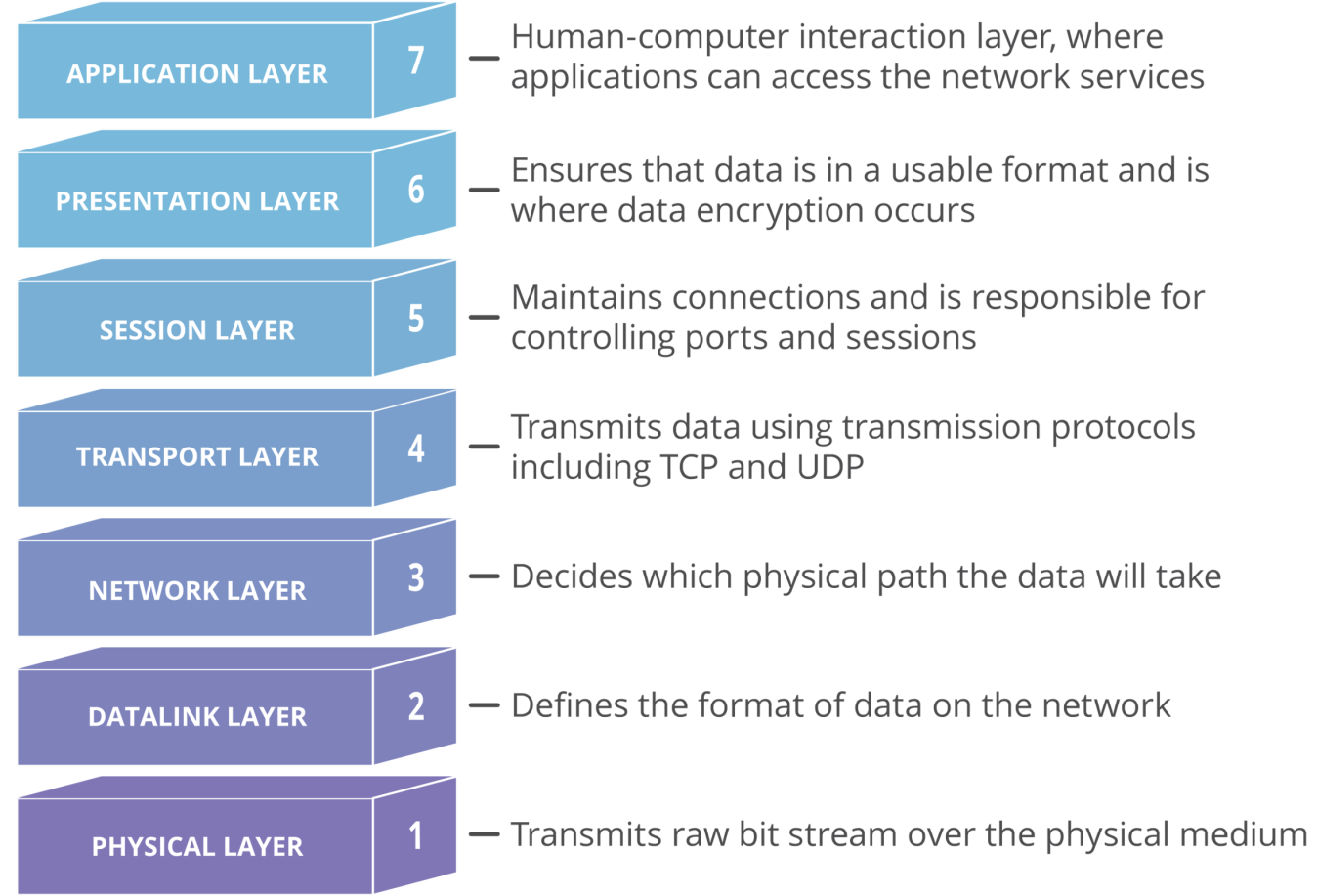
**Figure 3.1 How does DDOS Attack Work   
(https://www.cloudflare.com/img/learning/ddos/what-is-a-ddos-attack/ddos-attack-traffic-metaphor.png)**

A DDoS attack requires an attacker to gain control of a network of online machines in order to carry out an attack. Computers and other machines (such as IoT devices) are infected with malware, turning each one into a bot (or zombie). The attacker then has remote control over the group of bots, which is called a botnet.

Once a botnet has been established, the attacker is able to direct the machines by sending updated instructions to each bot via a method of remote control. When the IP address of a victim is targeted by the botnet, each bot will respond by sending requests to the target, potentially causing the targeted server or network to overflow capacity, resulting in a denial-of-service to normal traffic. Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

**3.1.1 Common types of DDos attacks**

Different DDoS attack vectors target varying components of a network connection. In order to understand how different DDoS attacks work, it is necessary to know how a network connection is made. A network connection on the Internet is composed of many different components or “layers”. Like building a house from the ground up, each step in the model has a different purpose. The OSI model, shown below, is a conceptual framework used to describe network connectivity in 7 distinct layers.



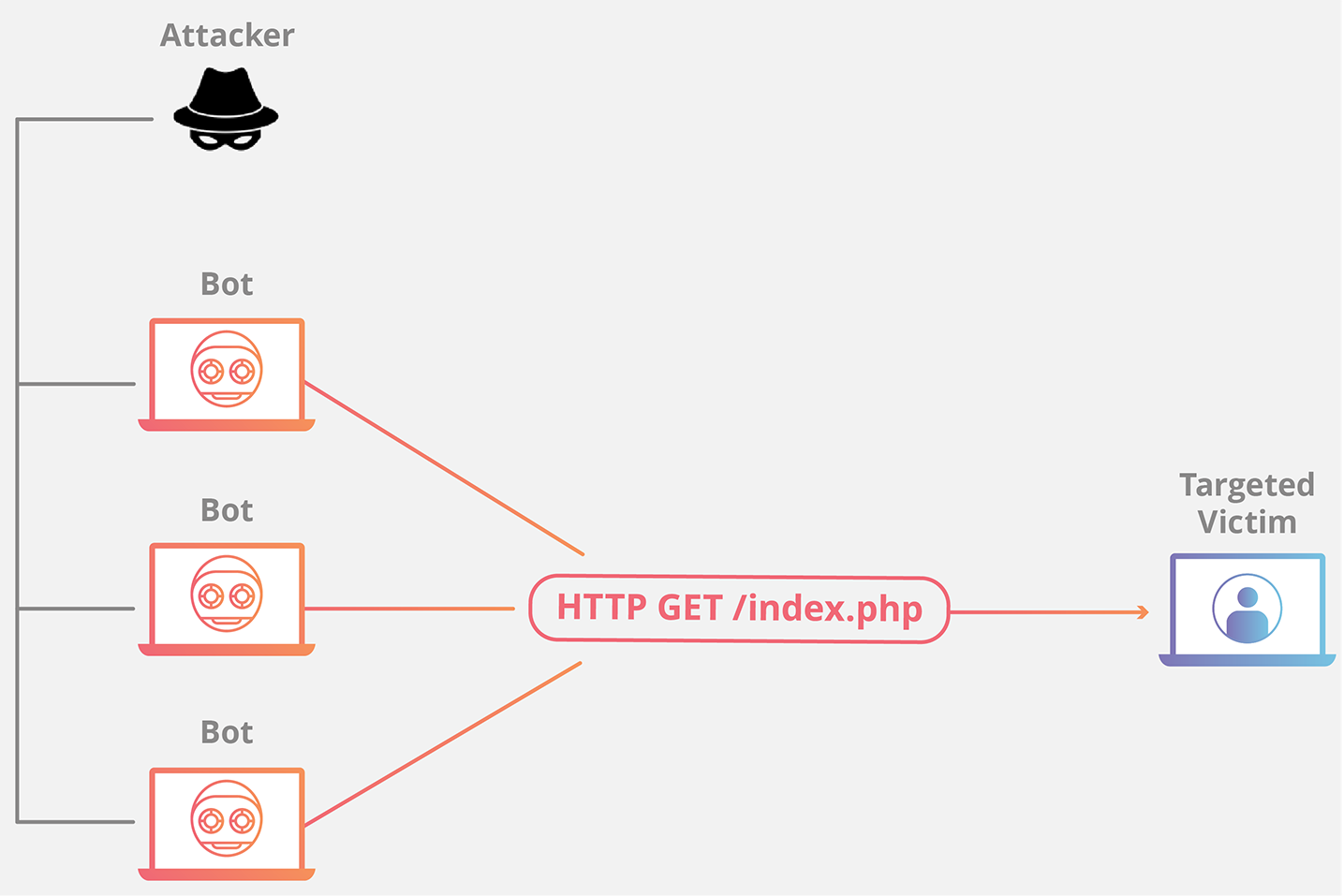
**Figure 3.2 Common Types of DDOS Attack  
(https://www.cloudflare.com/img/learning/ddos/what-is-a-ddos-attack/osi-model-7-layers.svg)**

While nearly all DDoS attacks involve overwhelming a target device or network with traffic, attacks can be divided into three categories. An attacker may make use one or multiple different attack vectors, or cycle attack vectors potentially based on counter measures taken by the target.

**3.1.2 Types of DDoS Attacks**

A. Application Layer Attacks

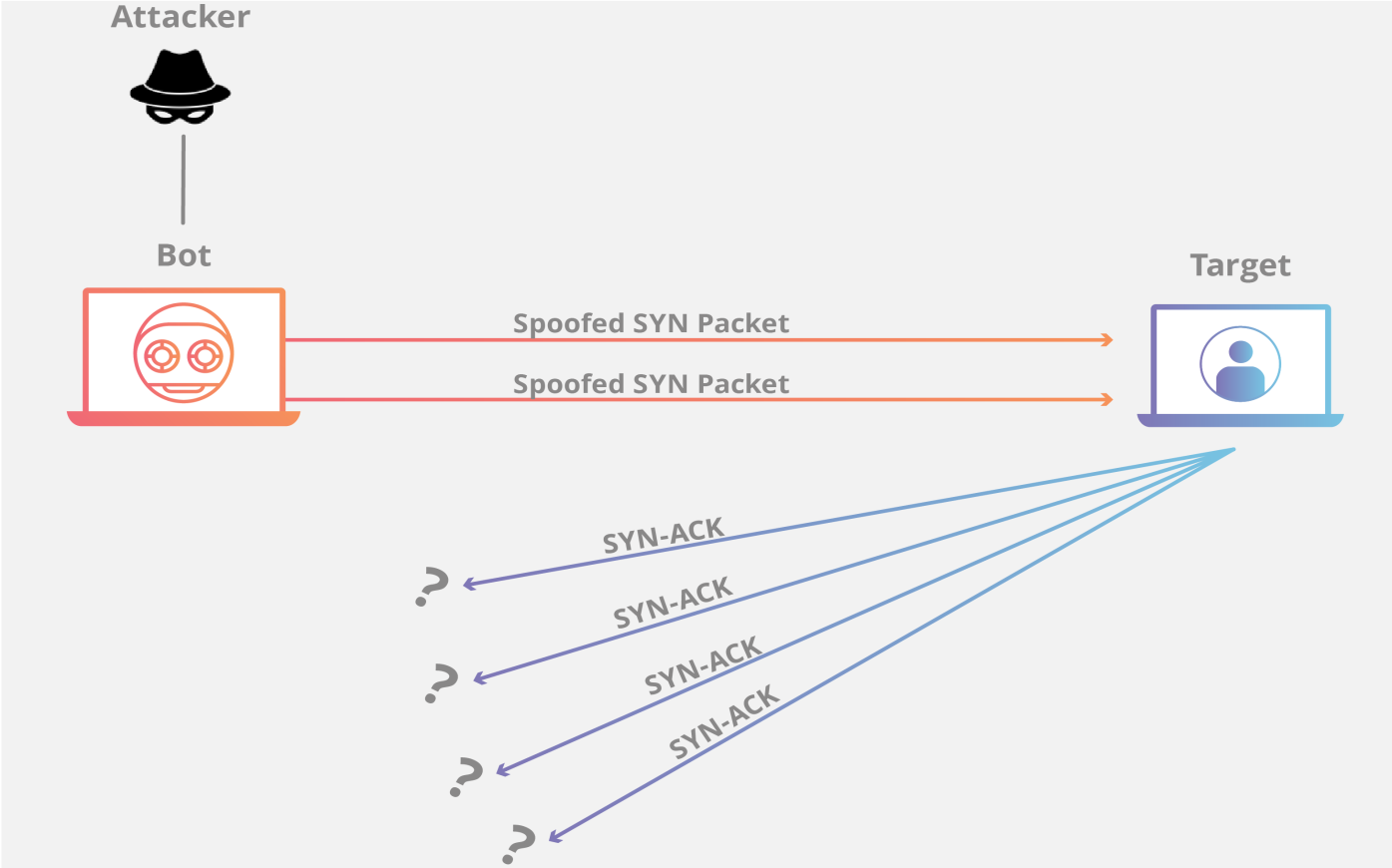
Sometimes referred to as a layer 7 DDoS attack (in reference to the 7th layer of the OSI model), the goal of these attacks is to exhaust the resources of the target. The attacks target the layer where web pages are generated on the server and delivered in response to HTTP requests. Layer 7 attacks are difficult to defend as the traffic can be difficult to flag as malicious.



**Figure 3.3 Application Layer Attacks  
(https://www.cloudflare.com/img/learning/ddos/what-is-a-ddos-attack/http-flood-ddos-attack.png)**

B. Protocol Attacks

Protocol attacks, also known as a state-exhaustion attack, cause a service disruption by consuming all the available state table capacity of web application servers or intermediate resources like firewalls and load balancers. Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible.



**Figure 3.4 SYN Flood**

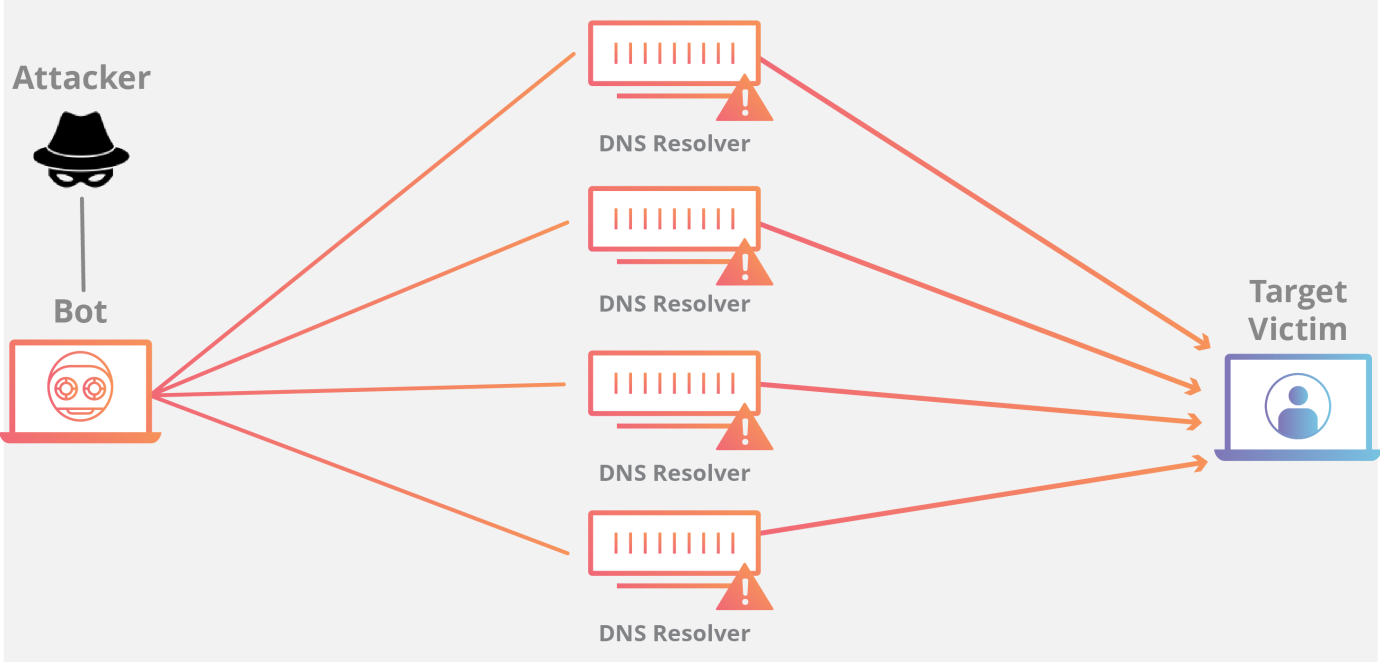
**(https://www.cloudflare.com/img/learning/ddos/what-is-a-ddos-attack/syn-flood-ddos-attack.png)**

SYN Flood

A SYN Flood is analogous to a worker in a supply room receiving requests from the front of the store. The worker receives a request, goes and gets the package, and waits for confirmation before bringing the package out front. This attack exploits the TCP handshake by sending a target a large number of TCP “Initial Connection Request” SYN packets with spoofed source IP addresses.

C. Volumetric Attacks

This category of attacks attempts to create congestion by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.



**Figure 3.5 DNS Amplification**

**(https://www.cloudflare.com/img/learning/ddos/what-is-a-ddos-attack/ntp-amplification-botnet-ddos-attack.png)**

DNS Amplification

By making a request to an open DNS server with a spoofed IP address (the real IP address of the target), the target IP address then receives a response from the server. The attacker structures the request such that the DNS server responds to the target with a large amount of data. As a result, the target receives an amplification of the attacker’s initial query.

**3.1.3 Example DDoS Attack Tools**

These are just a few examples of DDoS attack tools:

A. Low Orbit Ion Cannon (LOIC)

The Low Orbit Ion Cannon is a tool commonly used to launch DoS and DDoS attacks. It was originally developed by Praetox Technology as a network stress-testing application, but it has since become open-source and is now mostly used with malicious intent.

This tool puts the ability to launch DDoS attacks in the hands of users with very little technical knowledge. It is widely available for download and has a simple point-and-click interface, additionally users can even launch attacks from a web browser using a JavaScript version called JS LOIC and a web version known as the Low Orbit Web Cannon.

B. What is the High Orbit Ion Cannon (HOIC)?

The High Orbit Ion Cannon is a popular tool used to launch DoS and DDoS attacks, which aims to flood a victim's network with web traffic and shut down a web site or service. It's an easily available piece of open-source software developed by the Anonymous hacktivist group, and it's a successor to an older DDoS tool called the Low Orbit Ion Cannon (both named after sci-fi video game weapons).

Although it is used in many malicious and illegal attacks, the HOIC is still legally available because it has applications as a legitimate testing tool for users who want to implement a "stress test" on their own networks.

**3.2 How DDoS Mitigation Works**

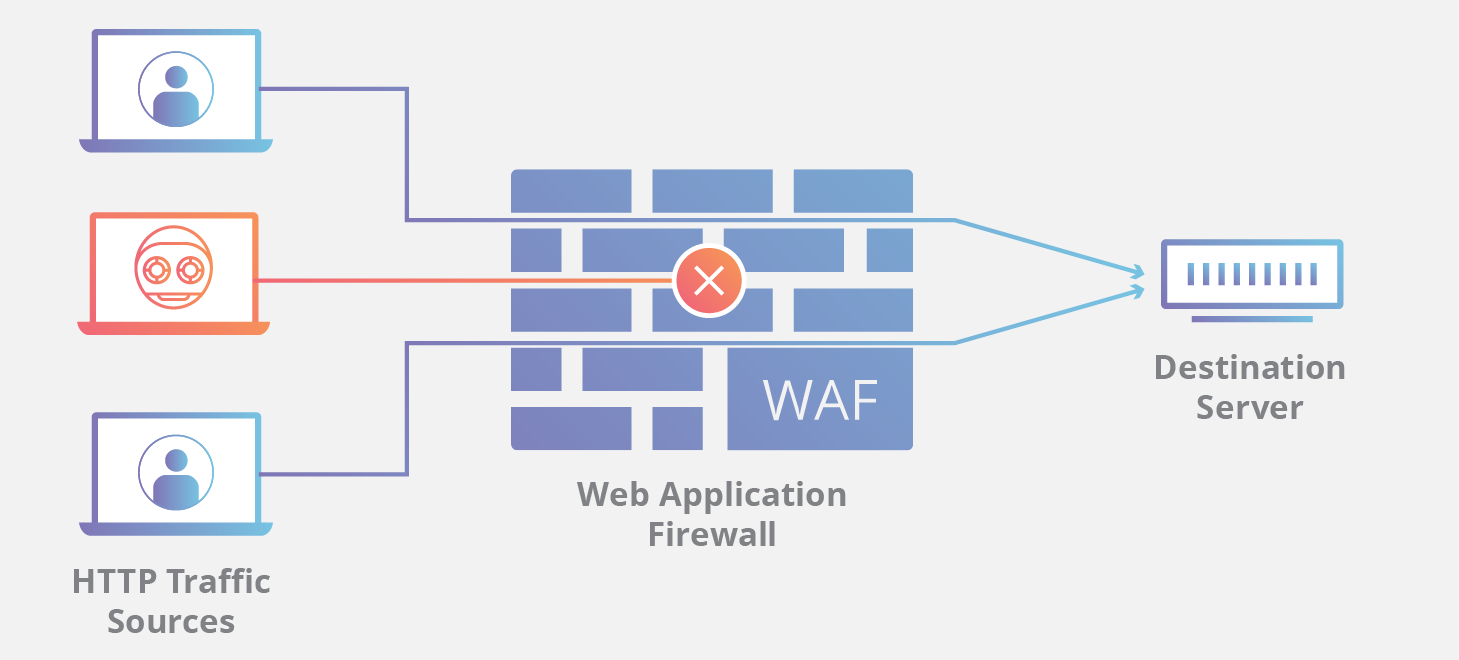
DDoS mitigation systems work mainly by inspecting different aspects of the traffic. Many systems keep track, as an aggregate, the amount of traffic to a destination IP or network and compare that to historical averages to see if 'too much' traffic is coming in or 'traffic is nearing a maximum level' for a pipe. Systems then tend to keep models at the source\_ip level, recording how much traffic they are seeing from a source. Traffic is broadly measured in PPS (packetsper second) and BPS (bits per second). Again this tends to be compared against historical averages.

The DDoS attack mitigation solution works by diverting DDoS traffic in one of the outer layers - the network layer. This helps to absorb any potential DDoS application layer traffic at the edge of the network. This means that threats can be prevented in the cloud before reaching the customer's origin. Web Application Firewall (WAF). WAF provides additional protection against these deeper application layer attacks in HTTP and HTTPS traffic.

**3.2.1 Method DDoS Mitigation**

Web Application Firewall

A Web Application Firewall (WAF) is a tool that can assist in mitigating a layer 7 DDoS attack. By putting a WAF between the Internet and an origin server, the WAF may act as a reverse proxy, protecting the targeted server from certain types of malicious traffic. By filtering requests based on a series of rules used to identify DDoS tools, layer 7 attacks can be impeded. One key value of an effective WAF is the ability to quickly implement custom rules in response to an attack. Learn about Cloudflare's WAF

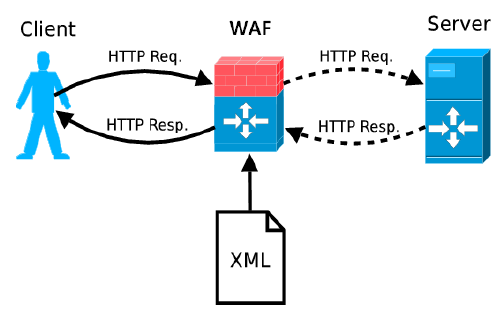


**Figure 3.6 Web Application Firewall**

**(https://www.cloudflare.com/img/learning/ddos/glossary/waf/waf.png)**

A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defense (in the OSI model) and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools that together create a holistic defense against a range of attack vectors

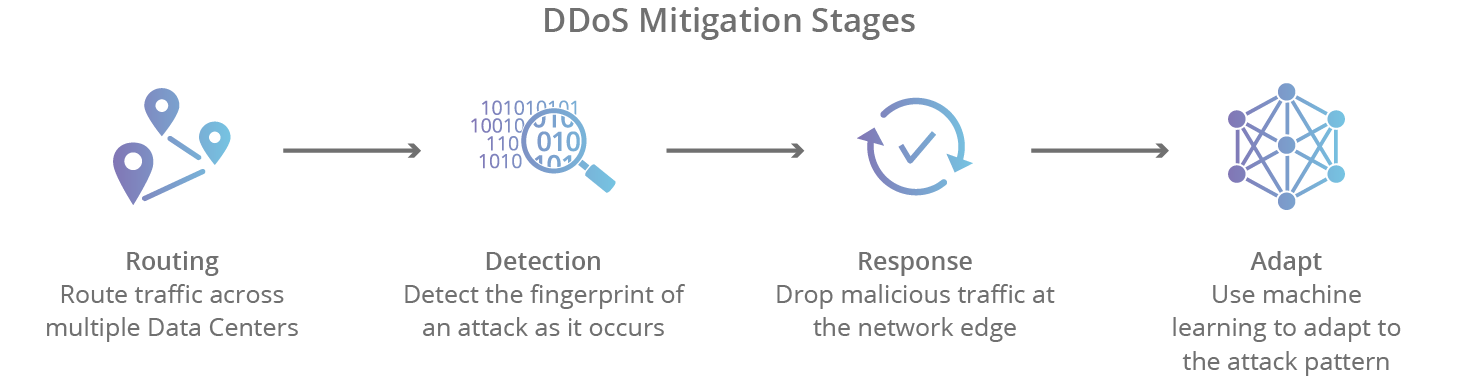
**3.3 An Architecture for Web Application Firewall**



**Figure 3.7 Architecture WAF**

**(**[**https://www.researchgate.net/figure/Web-Application-Firewall-architecture\_fig1\_267414465**](https://www.researchgate.net/figure/Web-Application-Firewall-architecture_fig1_267414465)**)**

Our WAF analyzes HTTP requests sent by a client browser trying to get access to a web server. The analysis takes place exclusively at the application layer. The system follows the anomaly-based approach, detecting known and unknown web attacks, in contrast with existing signature-based WAFs. In our architecture, the system operates as a proxy located between the client and the webserver. Likewise, the system might be embedded as a module within the server. However, the first approach enjoys the advantage of being independent of the web platform.



**Figure 3.8 DDOS Mitigation**

**(https://www.cloudflare.com/img/learning/ddos/ddos-mitigation/ddos-mitigation-stages.png)**

There are 4 stages of mitigating a DDoS attack using a cloud-based provider:

1. Detection - in order to stop a distributed attack, a website needs to be able to distinguish an attack from a high volume of normal traffic. If a product release or other announcement has a website swamped with legitimate new visitors, the last thing the site wants to do is throttle them or otherwise stop them from viewing the content of the website.

2. Response - in this step, the DDoS protection network responds to an incoming identified threat by intelligently dropping malicious bot traffic, and absorbing the rest of the traffic. Using WAF page rules for application layer (L7) attacks, or another filtration process to handle lower-level (L3/L4) attacks such as Memcached or NTP amplification, a network is able to mitigate the attempt at disruption.

3. Routing - By intelligently routing traffic, an effective DDoS mitigation solution will break the remaining traffic into manageable chunks preventing denial-of-service.

4. Adaptation - A good network analyzes traffic for patterns such as repeating offending IP blocks, particular attacks coming from certain countries, or particular protocols being used improperly. By adapting to attack patterns, a protection service can harden itself against future attacks.

**CHAPTER IV**

**CONCLUSION AND SUGGESTION**

1. **Conclusion**

DDoS attacks will develop increasingly sophisticated and massive capacity. Currently protected is even greater because it can ride IoT devices online. Therefore, the required hybrids are needed. Moreover, the current attack can quickly enlarge, quickly someone to conquer the company's operational system - making their applications inaccessible and also various useful information. For this reason, security solutions must be sufficient to support current challenges in terms of capabilities and also be able to optimize hybrid ecosystems while mitigating DDoS compilation attacks as they attack networks.

1. **Suggestion**

We recommend to be more careful in computer network systems, and we recommend that you always use a security protection system to prevent attacks on networks such as this and always follow the development of any security system in the world to always be safe.

# Bibliography

**1.D.Keromytis,Angelos.**2003. https://www1.cs.columbia.edu/~angelos/Papers/jsac-sos.pdf [02/03/2020]

**2. Sharma,Kapil**.2017. https://medium.com/@kapil.sharma91812/understanding-ddos-attack-15dd2cbce2a [02/04/2020]

**3. Sundaram,Meenakshi**.2019. https://medium.com/datadriveninvestor/ddos-attack-explained-9d67d467b1aa [02/04/2020]

**4.** https://www.f5.com/pdf/products/ddos-hybrid-defender-overview.pdf [04/03/2020]

**5.** https://www.cloudflare.com/learning/ddos/ddos-mitigation/ [06/03/2020]

**6.Alvarez,Gonzales.**2017.https://www.researchgate.net/publication/267414465\_An\_Anomaly-Based\_Approach\_for\_Intrusion\_Detection\_in\_Web\_Traffic#pf4 [09/03/2020]

**7.** https://www.e2enetworks.com/help/glossary/waf-web-application-firewall/ [09/03/2020]