2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS) | 979-8-3503-2045-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/IOTSMS58070.2022.10062168

An Overview of Defense Techniques Against DoS Attacks

Muhammad Afzaal
College of Engineering
AlAin University
AlAin, United Arab Emirates
muhammad.afzaal@aau.ac.ae
ORCID: 0000-0002-4559-993X

***Abstract*— Denial of Service (DoS) attack is a common type of cyberwarfare and as the name shows that its basic purpose is to stop services for legitimate users. It is different from hacking something such as unauthorized access, steal sensitive information, or leak information, etc. Our research provides the historical attacks, prediction, and types of DoS as well as its defenses. There are different defense mechanisms for several DoS attacks. We categorize these tools and techniques into two types i.e. client-side defense and server-side defense. So, the server-side defense tools are more effective and convenient but client-side defenses are difficult to deploy to the whole world. However, this is very important for identifying, mitigating, and preventing the DoS attacks for national and commercial security.**

Keywords— DoS Attacks, Denial of Services Attacks, DoS Attacks Preventive Measures, Denial Services Attacks Preventions, DDoS Attack

I. INTRODUCTION

Denial of Service (DoS) attack is a cyber-attack in the computer world, in which the attacker tries to temporarily interrupt or suspend the services of a device connected to the server/Internet to make a computer or network resource inaccessible to its legitimate users. For example, whenever an attacker targets a web server and sends malicious traffic continuously and prevent some or all real users to get access to the network services. After a couple of minutes, flooding the large volume of traffic overload the victim server and it gets crashed.

Attackers mostly target major companies like Banks, eCommerce, Media Channel, Government, Trading Companies, etc. to shut down their machines or network for making it inaccessible to its intended users. It is one of the oldest techniques of cyber extortion attacks to target victims. DoS attacks are not intended to steal information or damage assets but only target victims to destroy networks or services to legitimate users.

A Distributed Denial of Service (DDoS) is one of a popular type of attack that is most serious, dangerous, and difficult to identify [1]. It is a large-scale attack that prevents a legitimate user to grant services. An attacker adopts many unique IP addresses or computers that are mostly from thousands of malware-infected hosts. It is a malicious attempt to overburden the victim with the flood of online traffic to interrupt the usual traffic of a targeted network or server. A DDoS requires an attacker to access control of an online computer on the network, each computer is infected with malware and turning into a bot (like zombies). It has remote access control to the group of bots (botnet). Botnet is a portmanteau of words "robot" and "network" but unfortunately it is used in negative or malicious definitions. After the setting up of a botnet, the attacker can send instructions to botnet directly through a remote-control system. For further complicating identifying and defeating the attack, an attacker may involve IP address spoofing. As a bot is a legitimate user, the normal traffic can cause the overwhelming and slowing down the server ever it crashes.

II. TYPES OF DOS ATTACKS

A. Application Layer Attack

As the term indicates, the Application Layer attack on layer 5 via layer 7 in the OSI model such as FTP, SMTP, HTTP, HTTPs, TLS, and also VoIP applications [2]. These attacks are designed to target the application itself, the most common web server, and can also target SIP voice services and BGP. Application Layer or layer 7 attack is the most different malicious type from an entire network attack to target the top layer of OSI Model where the internet requests like GET and POST of HTTP are generated. These attacks frequently target financial institutions (i.e. retail and commerce banks, internet banking, investment banks, brokerage firms, and insurance companies), security staff, etc. especially for an application layer attack like a botnet that attacks an HTTP Flood server.

B. Reflection Attack

The reflection attack is executed in which the attackers spoof source address of exact target system and send packets to a known intermediate devices [3]. The response is sent to the target system when the intermediate devices respond. Actually, it reflects an attack from the intermediary called a reflector and therefore it is referred to as a reflection attack. The attacker generates a response packet that is larger than the original request by using a service. An attacker is able to transform a smaller packet flow from the network into a larger packet flow and intermediary directed at the target system. For this intension, The UDP services are commonly used. Actual echo service does not produce a high-volume response packet but it was a preferred option but for such an attack any UDP service that is commonly applicable can be used.

The intermediaries are usually selected to network servers with high capacity and routers with excellent network connections to produce high volume traffic. If the high-volume traffic is not necessary, an attacker can blur normal high volumes of traffic across them. When the attacker executes the attack cyclically over many intermediary systems, it may not be easy to differentiate the attack traffic flow from the other traffic flowing in the system. In combination by the use of spoofed source IP address, the complexity of any attempt to trace packet flows back to the system of the attacker is greatly increased.

This attack can only be detected and blocked when an intrusion detection is running to detect a very large number of failed link requests from the system. When the attacker is using many intermediaries, a few ones may identify and prevent the attack but mostly are not able to detect and the attacker will still succeed. A normal DNS operation showed in upper part and lower part is an example of attack flow (see Figure 1).

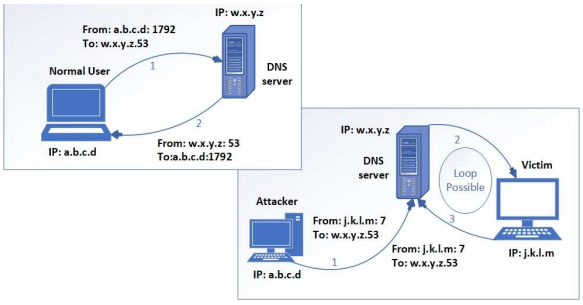

Fig. 1. Process of a normal flow and Reflection Attack

In normal traffic, the user sends a query to the 53 port from its port of UDP 1792 to receive the IP address of the domain name and the UDP packet and IP address of the DNS server responds. In DNS reflection attack, the attacker passes the query with the spoofed source address (of victim IP "j.k.l.m") to DNS server. The attacker uses a reflecting service (port 7) that is normally connected with echo. So, the DNS server sends the victim address, j.k.l.m to port 7. It may produce packets that echo the retrieved data return to the DNS server if the echo service is offered by the victim and caused the DNS server to loop with the victim machine/network if the DNS server is responding to the victim. Most firewall rulesets either host-based or network-based prevented suspicious source and destination ports variations.

C. *Amplification Attack*

The amplification attacks are different form of reflector attacks that include delivering for the victim device, a packet with spoofed source address to intermediary systems [3]. They separate where multiple response packets are produced in every actual packet. This can be done by routing the real request towards any network broadcast address. In this way, every host in this network will respond to the request and produce a flood of replies (see Figure 2). A service handled by many hosts on the intermediate network must only be used.

The enhanced protection against this kind of attack is that directed broadcasts cannot be transmitted from outside to a network. This is, in fact, another longstanding recommendation for protection that has been common as the suggestion for blocking fake source addresses. These attacks cannot work if such mechanisms of filtering are in existence.

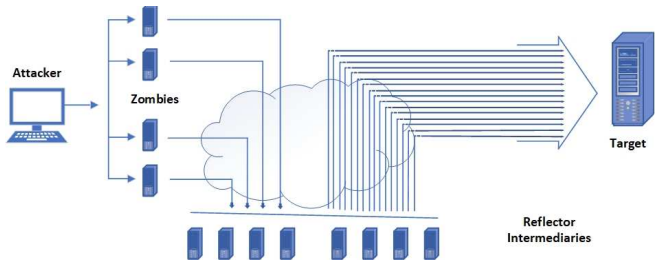

Fig. 2. Process of Amplification Attack

Another protection is to prevent access from outside to the network services like echo and ping. This prevents the use of networks in these attacks, at a convenient cost to analyze certain legitimate network concerns. Cybercriminals (attacker or hacker) scan the Network in search of well-connected networks that allow direct broadcasting and reflect accurate services. These lists are marketed and used for attacks.

D. *E-Mail Bomb Attack*

E-Mail Bombs are a type of Denial-of-Service (DoS) attacks that are an attempt to send a huge number of spam emails to overload email system [4]. Victims face a massive volume of messages that fill up their inbox instantly when the attack begins. The attack makes the mailbox of the victim useless in sufficient quantity. Attackers mostly used newsletter and signup forms from normal websites to target victims. Remember that TCP operations will not be used in these attacks and they cannot be aimed at a broadcasting address because they are connection-oriented.

E. *Zero-Day DDoS Attack*

The word Zero-Day or 0-day attack is typically used for attacks that exploit new vulnerabilities in security systems that the world has yet been unaware of [5]. The vulnerability can be detected for sure a long time until the new patch is released and installed. The vulnerability is being effectively used in this time to block resources and steal information. The hacker can assemble a successful DDoS attack in a short time, ideally through non-discredited servers. The strategies of 0-Day vulnerability are an ideal option. That is why hackers everywhere in the globe get more and more famous. For their goal to be reached, the malicious users must have access to a Zero-Day vulnerability application server. The server can then be used to attack this kind.

III. Historical Attacks

Some of the most impressive DoS attacks to date have been studied here to give you a sense of how catastrophic these attacks are. On average 28,000+ actual DoS attacks take effect every day [6].

A. *DDoS Using Trin00*

A sudden attack occurred on 22 July 1999 from the machines infected by a malicious script called Trin00 on a University of Minnesota on that day [7]. This code caused corrupted machines to send superfluous data packs to the

university to overload their computer and prevent legitimate requests from being processed. The assault therefore knocked the machine out for two days. This was a first Distributed Denial of Service (DDoS) attack to be spread across the world. Yahoo was a major victim of this attack.

B. DoS Attack using Mirai

Panix (3rd oldest ISP in the world) went unavailable for a few days by the flood attack [8]. It was the first publicly and documented DDoS attack that launched in September 1996. Different mail, news, name, and web servers are targeted as well as user "login" machines on ISP network. As the SYN flood attack used to play out available network links which stop valid users to connect Panix ISP servers. An international community of Internet experts took about 36 hours of efficient research to gain control of the Panix domains and servers.

C. Attack on GitHub

On 28 February, 2018, famous software developers' platform known as GitHub, had suffered a DDoS attack, which lasted approximately 20 minutes and clocked 1.35 terabits per second. According to GitHub, "over a thousand separate autonomous system numbers (ASNs) across tens of thousands of specific end points" have been reached by traffic. GitHub explains: "We deployed additional transit to our facilities last year in the incident report of the organization. During that time, we more than doubled the transit capacity which helped us to resist some volumetric attacks without affect to the user. However, attacks like these also need partner help for blocking and filtering of larger transmission networks. The attack on GitHub was noticeable as the attack was executed using a normal instruction of the database-acceleration cache program Memcached. The attack technique from Memcached DDoS has an especially effective amplification factor of up to 51,200 times the ratio between the request size of attacker and the DDoS attack traffic amount produced.

D. DDos Attack on Amazon

Amazon Web Services was hit by a huge DDoS attack in February 2020 [7]. It targeted AWS customer with CLDAP Reflexion technology. The technology is based on vulnerable CLDAP servers from third parties and enhance the amount of data sent 56-70 times to the IP address of the victim. The attack lasted three days, reaching a peak of 2.3 terabytes per second. The impact and consequences of the attack on AWS clients hosting prospective financial losses and brand casualties were major, although the interruption of AWS DDoS attack might be less serious than could be.

IV. Purpose And Scope

In an attempt to detect intelligent attacks, the detection of anomalies in Internet traffic has become very important, as the number of attacks on network infrastructure increases rapidly. DoS attacks have become a major security challenge to the Internet community. DoS attacks prevent valid customers of a network, including websites and computer systems, from using the services. The attack happens when a malicious attacker tries to use all available resources to block all services that legitimate users want to use. In such cases, the attacker often uses disc space, memory as well as CPU besides bandwidth consumption. The server gets overloaded by traffic, which prevents legitimate users from responding to countermeasures. Distributed Denial of Service attacks are launched indirectly through compromised devices, which enable organized network/system attacks. For instance, the DDoS attack can overwhelm web servers by continuously sending the data beyond their handling functions This attack aims to interrupt the targeted system by using Internet concepts and thus overwhelms legitimate users by preventing them from service access. The hacker guarantees that there is more traffic generated than the victim can handle, thereby allowing it to manage the distributed attack, obtaining as many computers as possible. These attacks need to be detected, handled, and prevented and looked at how malicious and legitimate users can distinguish from each other, as they are a popular growing issue facing to date. The development of a comprehensive solution that requires a range of security activities to trap various DDoS attacks is promising guidance. If one defensive level fails, others also can shield themselves from attacks.

A. Cisco Prediction for 2023

According to Cisco predictions (see Figure 3), the number of DDoS attacks will be raised to more than 15 million in the year of 2023 (from 7.9 million in 2018).

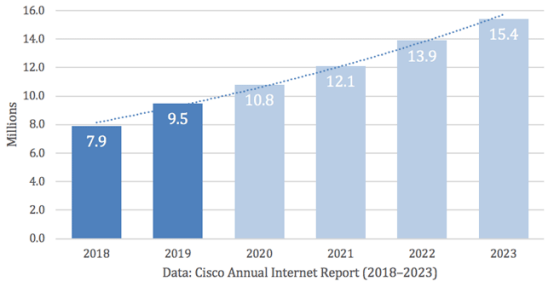

Fig. 3. History and predictions of DDoS total attacks by Cisco Systems[1]

The Cisco Systems provide an annual report in which measures digital transformation through various marketing divisions [9]. This report includes fixed broadband, wireless internet access, and mobile networking (3G, 4G, 5G). The increase in internet users, devices, and connections as well as performance is provided quantitatively.

Through 2023, almost 2/3 of the world population is predicted to access the Internet which will grow from 3.9 billion (51% of the world population in 2018) to 5.3 billion (66% of the world population). The world population upon the prediction of 2023 which compared to 2018, the total number of mobile subscribers will grow up to 5.7 billion (more than 71%) up from 5.1 billion (66%) and the total devices will be 3.6 (29.3 billion) per capita up from 2.4 (18.4 billion). Globally speed of Internet in 2023 up from 2018, the broadband will grow (more than double) to 110.4 Mbps up from 45.9 Mbps, Wi-Fi will grow (triple) to 92 Mbps up from 30.3 Mbps, and

[1] https://www.a10networks.com/blog/5-most-famous-ddos-attacks

mobile network will grow (more than triple) to 43.9 Mbps up from 13.2 Mbps.

A complete prediction report of 2023 year (see Figure 4). Population forecast is calculated from the United Nations, an analyst for the usage of broadband, hotspot, mobile, and business users from different sources.

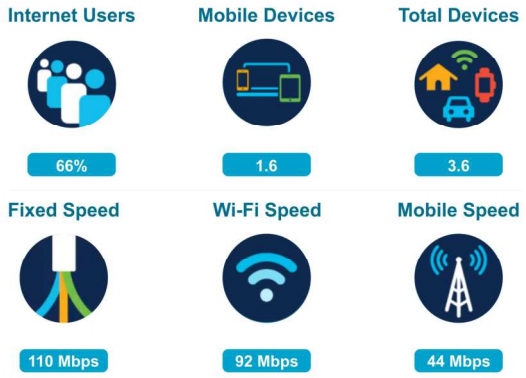

Fig. 4. Cisco Systems Future of digital transformation (2018-2023)[2]

V. Tools And Techniques To Defend Against DoS/DDoS

As the Internet Denial-of-Service attacks are practically challenging and difficult to prevent because the existing Internet protocol is not able to pre-verify packets before sending from source and authenticate after receiving at destination network by passing through inter-networks. Researchers and business people built private networks or mechanisms such as firewall or DMZ to ensure that the unwanted packet cannot pass without verification or authentication through the internet.

A. Client-side Defense

Firstly, we have to recognize the normal traffic in the network through some "traffic patterns" that detect and alert attack. It is also necessary to detect incoming traffic to separate traffic for legitimate users, bots, and hijacked web browsers. Secondly, it will be dropped or redirected as well as a threat is detected. DoS and DDoS attacks are launched against networks and websites of targeted victims. The anti-DDoS process can be done through different mechanisms and some of them are given below.

1) Ingress/Egress Filtering: Mostly attackers use spoofed/fake source IP addresses in DoS or DDoS attacks to produce a large volume of traffic from the medium network to the target machine [10]. In this case, a computer machine is also a victim of the attacker who belongs to a spoofed IP address. These filters are mostly implemented on the edge of routers (see Figure 5).

A packet that passes to the internet and arrives from the different routers must have an internal network source IP address. It is impossible to spoof any source IP address because of preventing packets with non-local source IP addresses from passing an interior network [11][12]. In real-time, each edge router in the network is capable of determining the source address of every packet and legitimate source address. We can understand it is the most feasible scheme in customer network but not recommendable for universal deployment due to administrative burden, router overhead, and challenges for current services based on spoofing of source IP address [13].

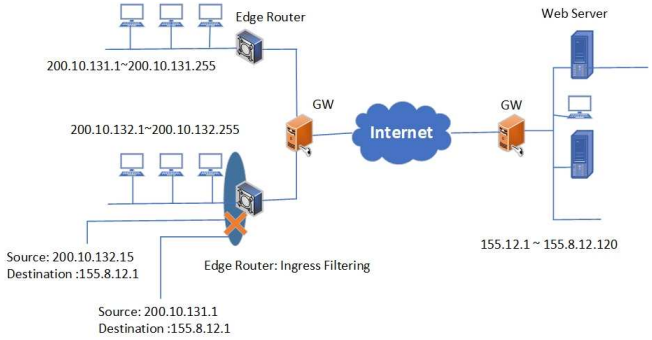

Fig. 5. Ingress / Egress Filtering Overview

2) IP Traceback: An IP Traceback technique normally begins from the nearest router of a victim and identifies the upload rate connections that generate malicious traffic. This method is uniquely executed repeatedly on the upstream router of network until the traffic source location is gained. As we can expect the attacker still there while the tracing process is done. There is practical network support for IP Traceback [14] (see Figure 6). Most of the attacks are shorter than 10 minutes that is why this technique is usually not useful in real-time tracing. One more disadvantage of this scheme is while the automated tool it creates massive overhead network system i.e. collecting packet data along with its routing paths and transmission in different ISPs routers.

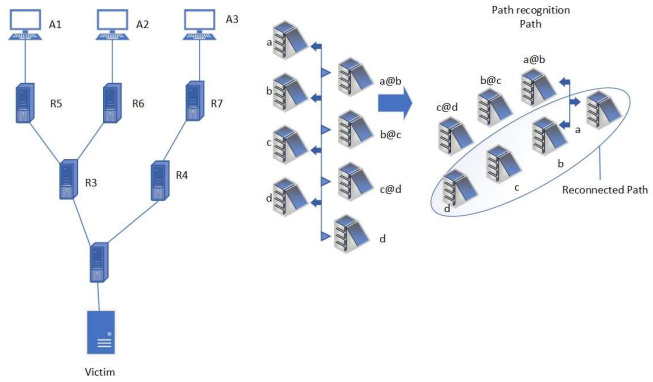

Fig. 6. Working of IP Traceback

As per defined proposal in which possibility of flood attacks tracing either marking packets or probabilistically with the address of their routers, victims use this marking material for tracing back to its source. In Fig. 6 left side define an attacking route (A2 > R6 > R3 > R1 > Victim), the right side is an

[2] https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/infographic-c82-741491.html

example demonstrates how the scheme can restore the whole map with the combination of routing characteristics.

3) Traffic Shaping: Nowadays, several routers have features that allow you to limit the flow of particular types of network packets. It is frequently known as "traffic shaping". In this technology data classification, quality of service, policy guidelines, queuing, and other techniques are used to ensure the bandwidth limit for voice and other important applications. This feature is called the Committed Access Rate (CAR) in the Cisco IOS application. A bandwidth set on network traffic correlates to an access list that can be enforced by CAR. In a DDoS attack, it may also be useful if you can build an access rule that suits any network traffic. For example, you can configure the system to restrict the bandwidth for specific types of packets to avoid attacks of ICMP or TCP SYN packets (see Figure 7). It will allow other packets to go through which may belong to the legitimate users network flow.

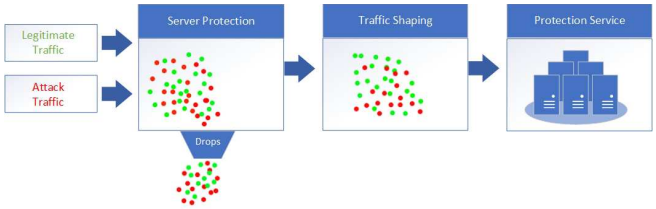

Fig. 7. Dropping packets that do not match access-list rules

4) Traffic Analysis: Researches proposed different methods by analyzing traffic patterns to prevent DDoS attacking packets and their characteristics. Many approaches used probabilistic and statistical analysis to identify the patterns of attacker packets or source. Mostly, the packets have a similar type of patterns that can be classified and a large-scale attack can also identify by rapid changes in the network traffic (see Figure 8). For example, initially select random samples, classify the selected packets, and then create a Database or normalize the data.

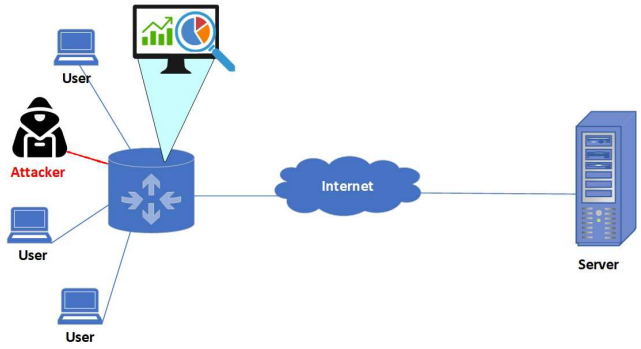

Fig. 8. Working of the Traffic Analysis defense tool

The majority of the common approaches are built in the second step such as the use of data mining [15], time series, and more complex mathematical models. As the systems depend on a probabilistic model, we cannot be fully confident that attacking packets will be identified or only illegitimate packets can be detected.

5) Authentication Header (IPv6): The researcher proposed an authentication header mechanism of IP version 6 to provide strong integrity and authentication for IP datagrams. As the previous methods such as Ingress/Egress Filtering, IP Traceback, Traffic Shaping, Traffic Analysis, and Host/Network Auditing are not secure enough to prevent DDoS attacks because of current features of IPv4. Since current Internet protocol version 4 has no specific technique for detecting legitimate packets, without any fear an attacker can use the in-active or spoofed IP source address.

Authentication Header (AH) is a new field of Internet Protocol version 6. AH provides message authentication and integrity to prevent spoofed IP addresses. Using IPv6, the AH header come after IPv6 and Hop-by-Hop/Routing headers (see Figure 9). It is generally used to encrypt IP packets and authenticate the source of the packets [16].

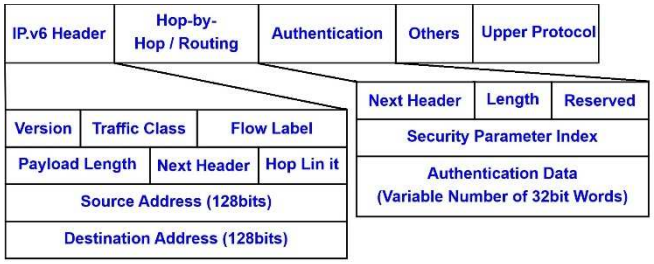

Fig. 9. Overview of Authentication Header

6) Active Cache: Active Cache is a simple method that keeps state info and basic functions queuing process on the routers [17]. There are two modules i.e. active DoS Attack Detection Module and DoS Attack Regulator Module. The Active DoS Attack Detection Module is capable to detect a large bandwidth attack flow based on cache Most Frequently Used (MFU) discipline. A trace notifier that applies the upstream limit of the router used by the DoS Attack Regulator Module through which the attack flow passes. It avoids other innocent flows from starving effectively. So, it is implemented above the "MAC" layer (see Figure 10) and do not change anything else. It is necessary to add “Data Structures” and its variables (i.e. “Packet Signature” and “Frequency_count”) in every router. Besides, a “drop_probability” variable is used to maintain data packets flow. This probability detects the attack flow by incremented multiplicatively and decremented linearly.

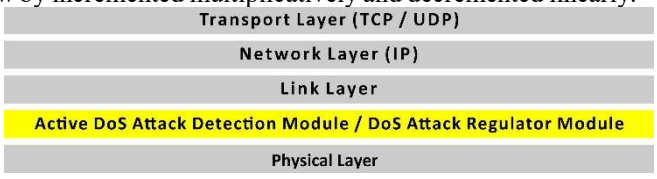

Fig. 10. Overview of active cache modules

In Active DoS Attack Detection Module, the existing packet signature is compared with the arrived packet signature in the cache. The frequency counter is incremented if the flow is already existing in the cache otherwise new entry is created in case of no found. A least count entry will be empty to maintain high-bandwidth flow when the cache memory is full. A network

attacker that continuously pumps network traffic should be labeled as an attack flow.

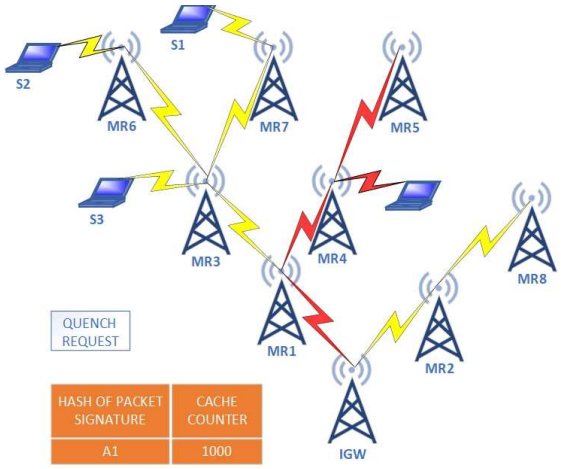

Fig. 11. Quench request of active cache method

In DoS Attack Regulator Module, an alert is sent to slow it after the attack traffic is detected. The module manages and controls the acceptance of an attack flow relying on a dynamic drop probability. As the drop probability reaches the maximum value, it considers attack packets and trace notifier sends a slowdown request to its upstream. As the drop probability reaches the maximum value, it considers attack packets and trace notifier gives the slowdown instructions to its upstream neighbor pumping packets (see Figure 11).

7) D-WARD:

As the Denial of Service is a worldwide threat in today internet society. We proposed a D-WARD method to automatically detect and stop the DDoS attacks by deploying mechanisms at the source-end network. Two-way traffic flows continuously monitoring to detect and stop these attacks. A predefined model is used to compare the normal traffic flow, store statistics values, and the rate-limit for mismatching aggressive flows (see Figure 12).

In this technique, we assure good service to legitimate users even attackers targeted the network. D-WARD has no memory to keep a record of previous attacks, an issue exists if attacks are repeated in defense against DDoS. Also, D-WARD unable to authenticate UDP attacks without spoofed source IP and high-rate flood. Hash-table may drop valid packets of legitimate users and provide poor service during the attack.

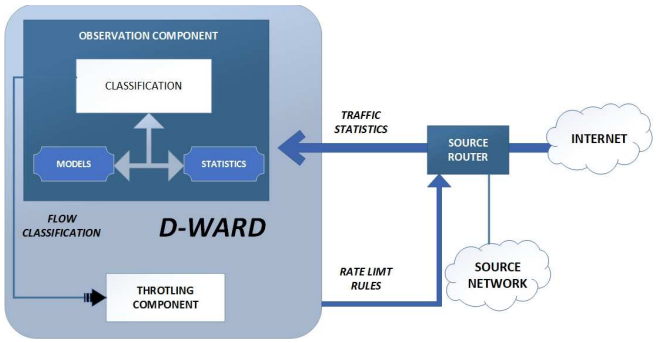

Fig. 12. A prototype for rate-limit before sending packets to destination

B. *Server-side Defense*

Without good protection tools and services, you cannot defend servers from online attackers. DDoS is one of the widest attacks that almost all kinds of organizations can experience today. Over the past three years, the frequency of threats by DDoS has grown more than double. We recommend some good anti-DDoS tools and platforms because these software packages are specially developed to prevent malicious traffic that is coming to the host system. These powerful tools detect threats through monitoring and stop various attacks including DoS and DDoS attacks.

1) Host/Network Auditing: Many DDoS scanning tools detect the presence of DDoS client and server binaries in the machine (see Figure 13). Different companies of Host audit tools have updated their products like antivirus tools developed or modified to include these signatures.

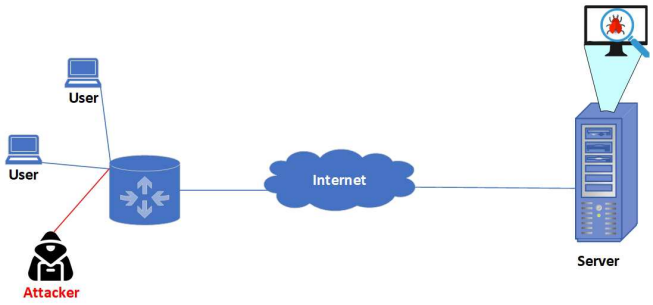

Fig. 13. Working of the Host/Network Audit tool

2) SolarWinds Security Event Manager: SolarWinds Security Event Manager has an event log management feature in the DDoS security tool [18]. Log files are an essential mechanism to identify unwanted users who are trying to interrupt a network. It keeps a list of suspected malicious users to defend yourself from threats so that the software automatically stops the IP from connecting with your host network (see Figure 14).

In case a malicious source transmits traffic, you can also configure alerts during an attack. DOS prevention and retrospective analysis can be performed through logs collected by SolarWinds Security Event manager. You can find profiles, IPs, or explore time intervals in more detail by sorting through the reports. It assists to enhance protection, reliability and solving problems by providing insightful reports and analysis.

Fig. 14. An Overview of the SolarWinds Security Event Manager and Logs

3) Sucuri Web Application Firewall: Sucuri Web Application Firewall (WAF) is a DDoS and zero-day exploits application server firewall [19]. The WAF protection and security identifies all traffic flows from HTTP / HTTPS and stops malicious traffic (see Figure 15). It blocks botnets from forcing your website offline. The firewall provides geo-blocking for further Sucuri WAF website.

Visitors from the top three countries with DDoS attacks are blocked via geo-filtering. However, you may have white list IP addresses that you trust to connect with your team, without being blocked, to control limited access. This is a cloud-based platform, which prevents hacks and stops attacks inside all websites. Our ongoing research enables us to identify and manage growing challenges and to implement your own decisions.

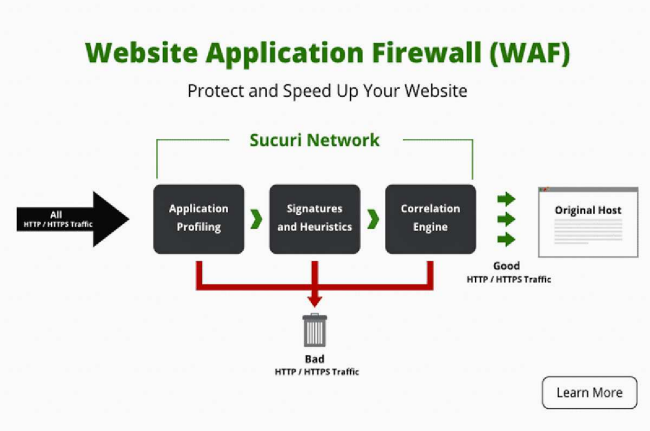

Fig. 15. A process of Sucuri Website Application Firewall

It defends website from malicious code and helps to prevent hacking. DDoS attacks can force to shut down server or site. We are blocking these attacks on layers 3, 4, and 7. Hackers every day discover new weaknesses. We safeguard websites and avoid concerns. Sometimes it just takes an update to prevent new threats. Most websites are attacked by automated hacker applications. Brute force and password breaks are avoided to prevent misuse of the website. It may implement strong passwords, CAPTCHA, 2FA, or IP whitelist. All traffic is investigated to block requests that do not fulfill the criteria of your system. When a malicious botnet or hacker tool is identified on our systems that attempt to target your website, it is automatically eliminated.

4) StackPath Web Application Firewall: StackPath is a web application firewall (WAF) and DDoS defense program built for protection from cybercriminals [19]. At layer 7, behavioral techniques are used for recognizing and blocking volumetric layer attacks. So, attacks like HTTP, UDP, and SYN floods are the protection capabilities program. StackPath has a capacity of 65 Tbps to tackle big threats (more than the highest record DDoS attack). The powerful attacks can be prevented by the available capacity (see Figure 16). It is also able to prevent attacks from anywhere in the world through its edge network. The StackPath WAF can be configured with DDoS limits to protect your applications from vulnerability. You may set DDoS thresholds to decide when an attack is being performed by the DDoS machine. For example, if the threshold of a server or a burst threshold exceeds a set of requests.

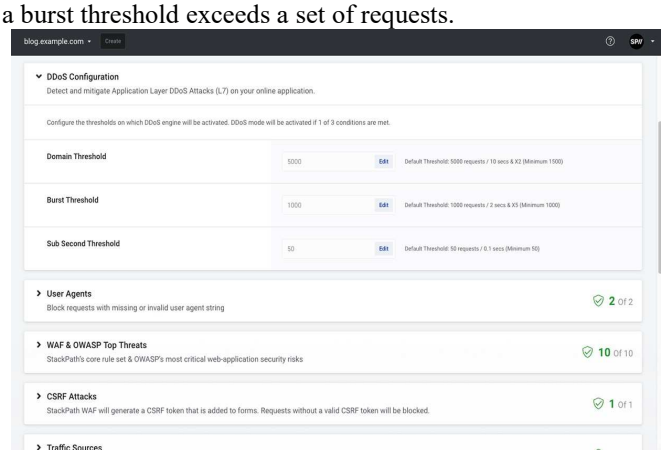

Fig. 16. An Interface of StackPath Website Application Firewall

5) Link11: Link11 is a DDoS defense tool based on the cloud. A device can recognize and prevent Web and DDoS attacks in real-time [19]. The program notices an attack by using artificial intelligence (AI). The AI explores and renders a correlation between the identified attack pattern sequences and such data. If a network connection interacts in the same way as a suspected attacker, then the system will reply directly via mobile text message whenever an attack is detected (see Figure 17).

It is very quick to use in terms of configuration as it is running within the cloud. You do not have to buy additional hardware and you can set up the program to secure the systems against attack. A central control view of the traffic, application, and server perform security services that can be provided via the dashboard to recognize and avoid threats. The simple implementation of AI and the dashboard offers a clear view of the performance of the server. A reporting capability also exists, so that you can get protection information. The feature enables you to plan or manually produce reports as per your demands. It is one of the most deployed DDoS security solutions because of its ease and automation.

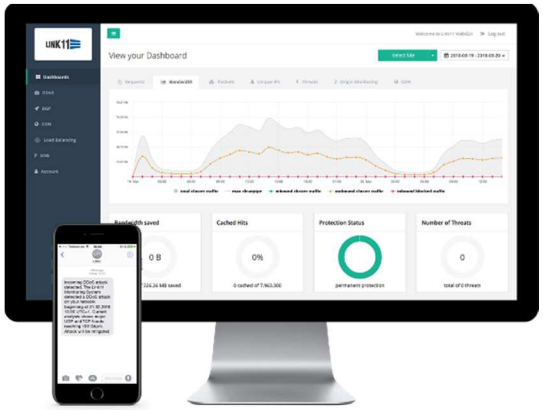

Fig. 17. Link11 dashboard and mobile SMS preview

The Border Gateway Protocol (BGP) will secure the largest organization networks with an IP network. As a fast shield or permanent version, the BGP defense is present. And the actual legitimate traffic flow continues until an attack is stopped. Traffic will be redirected to the filter center Link11 when an attack is detected, where it will be reviewed. Then a tunnel interface transfers the filtered data packets on to the organizational infrastructure. The client may decide whether to accept all traffic or an only specific part of traffic.

6) Cloudflare: Cloudflare is a high capacity DDoS defense tool which is 15x highest DDoS-attack ever recorded and has a 30 Tbps network capacity service [19]. Cloudflare can handle even the most effective attacks due to its high-performance. It uses an IP legitimacy database to detect new methods of attack.

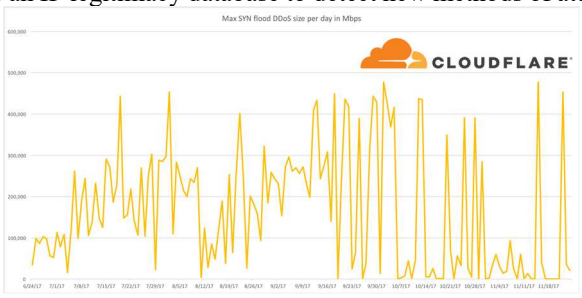

Fig. 18. DDoS SYN flood size per day

DDoS attacks against only Cloudflare customers every day are illustrated in the above chart (see Figure 18). However, it is necessary to keep in mind that this includes the attacks we identify. Cloudflare has also developed specific tools for customers to define what the threat looks like and how much traffic they think to treat.

Extended protection tools are worked out in Cloudflare under attack mode to assist reduce attacks of Layer 7 DDoS. Access to your site is verified for visitors and suspected traffic is restricted [27].

VI. Conclusion

Our research basically provides some common types of DoS attacks, history and also offers various tools and techniques for mitigation which were proposed by some researchers, scholars, organizations, etc. A few of defenses are client-side and mostly server-side because changing infrastructure on client-side is not only difficult but also costly. Anyhow, deploying some mechanism on client-side either edge router or ISP will not benefit because the router resources are not enough to handle a large volume of attack traffic. If any technique implemented on routers, they will be overwhelmed or for sure slow down routing. Nevertheless, a well-design infrastructure or defense system on server-side will be better for attack mitigation.

References

[1] Global Cybersecurity Leader - Palo Alto Networks, “What is a denial of service attack (DoS)?”, “https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos” , Last accessed on October 11, 2022

[2] Secplicity - Security Simplified, “Application Layer DoS Attacks”, "https://www.secplicity.org/2016/04/11/application-layer-dos-attacks/", Last accessed on October 11, 2022

[3] Stallings, W., Brown, L., Bauer, M. D., & Howard, M. (2012). Computer security: principles and practice (Vol. 2). Upper Saddle River: Pearson.

[4] Cybersecurity, Productivity and Compliance Solutions | AppRiver, “Email Bombs Disguise Fraud - Distributed Spam Distraction”, https://appriver.com/blog/email-bombs-disguise-fraudulent-activity, Last accessed on October 11, 2022

[5] DDoS-GUARD - DDoS Protection and Mitigation - Anti-DDoS, “Zero-day DDoS Attack (0day DDoS attack)”, "https://ddos-guard.net/en/terminology/attack_type/zero-day-ddos-attack-0day-ddos-attack", Last accessed on October 11, 2022.

[6] SecurityWeek- Information Security News, IT Security News and Cybersecurity Insights, “The Internet Sees Nearly 30,000 Distinct DoS Attacks Each Day: Study”, "https://www.securityweek.com/internet-sees-nearly-30000-distinct-dos-attacks-each-day-study", Last accessed on October 11, 2022.

[7] A10 Networks - Secure Cloud Application Services and Delivery, “Five Most Famous DDoS Attacks and Then Some”, "https://www.a10networks.com/blog/5-most-famous-ddos-attacks", Last accessed on October 11, 2022.

[8] GlobalDots - Web and Mobile Performance, Cloud Security and Cloud Performance Optimization, “15 Most Dangerous DDoS Attacks That Ever Happened”, "https://www.globaldots.com/blog/15-most-dangerous-ddos-attacks-that-ever-happened", Last accessed on October 11, 2022.

[9] Cisco Systems, Inc., “Cisco Annual Internet Report (2018–2023) White Paper”, "https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html", 25 August, 2020.

[10] Network Working Group, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", https://tools.ietf.org/html/rfc2827,.

[11] S. Savage, D. Wetherall, A. Karlin, and T. Anderson. Network support for IP traceback. IEEE/ACM Transactions on Networking, 9(3), June 2001.

[12] D. Moore, G. Voelker and S. Savage, “Inferring Internet Denial of Service Activity”, Proceedings of USENIX Security Symposium, 2001, August 2001.

[13] Goldreich O., “The Foundation of Cryptography: General Cryptographic Protocols,”Cambridge university press, Vol. 2, May 2004.

[14] Bao-Tung Wang, Henning Schulzrinne IRT, A DoS-Resistant IP Traceback Approach Columbia University

[15] J. Han and M. Kamber. Data Mining, Concepts and techniques. Morgan Kaufmann publishers, 2001

[16] Luis Rosello, “What is IPsec?”, SANS Security Essentials Practical Assignment Version 1.3, April 2002.

[17] Santhanam, Lakshmi, et al. "Active cache based defense against dos attacks in wireless mesh network." 2007 2nd International Symposium on Wireless Pervasive Computing. IEEE, 2007.

[18] Comparitech - Tech researched, compared and rated, “8 Best DDoS Protection Service Platforms & Anti DDoS Software”, "https://www.comparitech.com/net-admin/best-ddos-protection-service", Last accessed on October 11, 2022.

[19] Cloudflare - The Web Performance & Security Company, “Understanding Cloudflare Under Attack mode (advanced DDOS protection)”, "https://support.cloudflare.com/hc/en-us/articles/200170076-Understanding-Cloudflare-Under-Attack-mode-advanced-DDOS-protection", Last accessed on October 11, 2022.