Automatically defend from DoS and DDoS traffic flood attacks

Yinon Cohen and Maor Shabtay

Advisor: Dr. Amit Dvir

Ariel University

October 2017

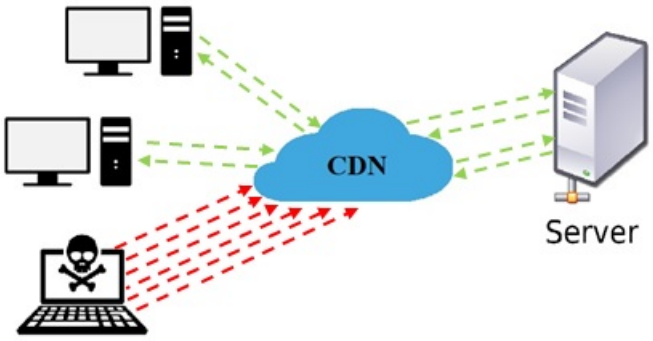
Contents

1. Abstract

Denial-of-service attack (DoS) and distributed denial-of-service attack (DDoS) attacks are attempts to exhaust server side assets, and designed to prevent client-to-server communication (denial of service). These attacks aim to both public and private sectors, and occur more and more frequently. In addition, lately the massive DDoS attacks are performing 100 Gigabits per second, and being more common than ever. These attacks are sowing fear among organizations and private server owners.

Our project deals with understanding and examining DoS and DDoS attacks, and what are the solutions for them. In particularly, we will discuss and handle with traffic flood attacks on web servers, and will try to develop our own software or algorithm to block or to give any immediately pragmatic solution.

Our main goal is to develop an automatic system that would identify and analyze a traffic flood attack, defend the server from it, and in need - will block any Internet Protocol (IP) or sub-net which the flood comes from. Our system should run on a Content delivery network (CDN) instead of on the server in order to save the server's performances providing service



2. Introduction

2.1. DoS

DoS attacks are attempts to exhaust server-side assets and designed to prevent client-to-server communication (denial of service). Simply, we can say that stealth server sabotage wires or even the server is denial of service, but in the context of data security we discuss about remote attacks and not physical sabotaging.

2.2. DDoS

DDoS attacks are very similar and sometimes even identical, and their intention is Distributed Denial of Service. In other words, the attack comes not from a single source, but from a large number of end stations – usually triggered by the attacker in the form of a king of virus located on these end stations. Most DDoS attacks are much more powerful and significant. It is important to understand that even an attack by two or three end stations is usually considered as a DoS attack, since there is really no significant flooding of the server.
Earlier this month Cisco released a white paper that [1] is part of the company's larger report, "Visual Networking Index Complete Forecast Update, 2015-2020." Here are some statistics from that white paper, relevant to distributed denial of service (DDoS) attacks:

- Frequency of distributed denial-of-service (DDoS) attacks has increased more than 2.5 times over the last 3 years.
- The average size of DDoS attacks is increasing steadily and approaching 1 Gbps, enough to take most organizations completely off line.
- Peak DDoS attack size (Gbps) is increasing in a linear trajectory, with peak attacks reaching 300, 400, and 500 Gbps respectively, in 2013, 2014, and 2015, at about 10 to 15 percent per year.
- In 2015 the top motivation behind DDoS attacks was criminals demonstrating attack capabilities, with gaming and criminal extortion attempts in second and third place, respectively.
- DDoS attacks account for more than 5 percent of all monthly gaming-related traffic and more than 30 percent of gaming traffic while they are occurring.
- Globally the number of DDoS attacks grew 25 percent in 2015 and will increase 2.6-fold to 17 million by 2020.

The DoS and DDoS attacks can be divided into two types:

- Attacks that flood and delay the service.
- Attacks that completely disrupt the service (and these we want to deal with in our project).

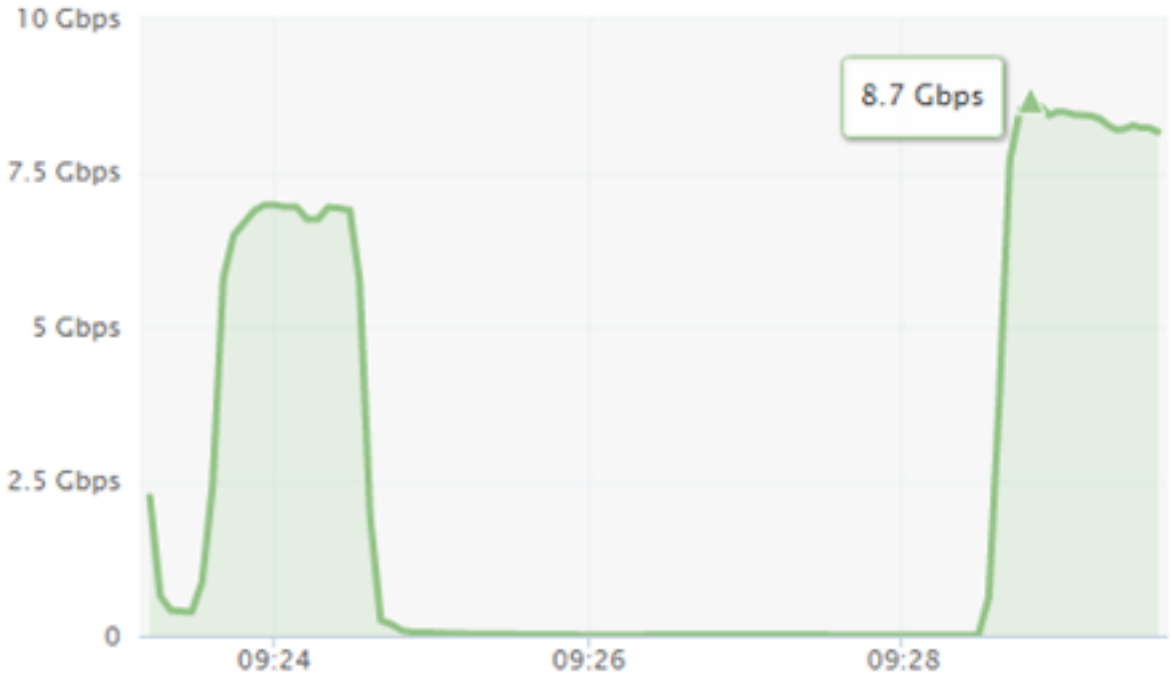


Figure 2.1: Sudden increase in server network traffic

2.3. DoS and DDoS attacks

Our research is including both types of attacks for DoS and DDoS attacks in general, and we will divide the types into different main types, based on the seven-layer-model (Open Systems Interconnection (OSI)) [2].

2.3.1. DoS and DDoS over Application layer

Attacks in the application layer are often generated by POST requests. They are also divided to sub protocols in the application layer – http / https.

- HTTP POST Flood - Creating and sending very large number of POST methods, to the extent that the server can't answer all requests, therefore service for real users of the server is compromised.
- HTTPS POST Flood - This is a flood of post methods that pass through Secure Sockets Layer (SSL) Session. The purpose of SSL is to take every message and decrypt it in order to inspect it. Flooding of these methods would harm the service.

- HTTP GET Flood - The attacker creates and sends to the server a huge amount of GET requests. The server needs to analyze all of them and return some data. Some people regard this attack as a Transport-layer attack, since sometimes the server would have to send a lot of data to the user attacker. Therefore, traffic and network bandwidth are flooded. Denial and service prevention depends on the server's capacity to getting and sending back packets. If it is able to handle a huge number of requests – the traffic will be damaged, and if it fails, the requests that it receives from real users will not be handled as the server falls.
- HTTPS GET Flood - Overflow of GET requests on HTTPS protocol requires a lot of work from SSL Session – decryption every message and hence load and sabotage the service.

2.3.2. DoS and DDoS over Transport layer

Flooding over Transport layer characterized mainly by packets that the server receives and is required to provide service – mostly by sending a requested data or any other response[2].

- Syn Flood - In this attack, the attacker takes advantage of the Transmission Control Protocol (TCP) principles that the server always wants to reach. When a server receives a Syn packet, it is a request from a client to open a connection, and it is obligated to respond to it and must return the client a Syn – Ack certificate. Each Syn message requires time from the server – analyzing the packet (understanding who created it, calculating 'Checksum' etc.), and then be able to reply. Therefore, flooding these messages is slowing down and compromising the server's serviceability.
- Rst Flood - Like Syn flood, the attacker takes advantage of TCP principles, including reliable communication. In case that a socket is closed or when one of the sides disconnected (and in few other situations), TCP has a solution. The connected side still wants to continue the communication (since there was no closing connection process), it sends a packet with a Rst flag and hence they have to re-open the connection. Like Syn packets overflowing, Rst packets overflowing also require a lot of work from the server and would sabotage the service.
- User Datagram Protocol (UDP) Flood - UDP floods are used frequently for larger bandwidth DDoS attacks because they are connectionless and it is easy to generate UDP messages from many different scripting and compiled languages. The attack can be initiated by sending a large number of UDP packets to random ports. As a result, the server would check for the application listening at that port, realize that no one is and reply with Internet Control Message Protocol (ICMP) packet saying 'Destination Unreachable'. Thus, for a large number of UDP packets, the server will be forced into sending many ICMP packets and much performance.

2.3.3. DoS and DDoS over Network layer

DoS and DDoS attacks over the Network layer are characterized with a large number of packets in order to overload the bandwidth and exhaust network resources. Network resources can be routers, firewalls and servers, and it is clear that their ability is final.

- ICMP Flood - ICMP protocol is typically used for error messages rather than data exchange between systems. Flooding messages with ICMP protocol – e.g. ping – is intended to overload the network.

2.3.4. DoS and DDoS over Link layer

DoS and DDoS attacks over the Network layer require access to the local network. Therefore, they are rare and more easy to detect.

- Media Access Control (MAC) Flood - A rare attack, in which the attacker has to be connected to the local switch. The attacker sends multiple dummy Ethernet frames, each with different invalid MAC address. Network switches maintaining their MAC table, and treating MAC addresses separately, and hence reserve some resources for each request. When all the memory in the table is used up, it either shuts down or becomes unresponsive.

2.3.5. Demonstrating APDoS Attack

The advanced persistent denial-of-servicel (APDoS) is an attack that combines many DoS and DDoS attacks, and is carried out by a lot of hostile elements over time. APDoS represents the worst Denial of Service attack that can occur. The idea behind it is a combination of many attacks from multiple endpoints, and over long period of time, hence its name Advances Persistent DoS. In this attack, the attackers usually attack several stations in order to create a distraction from the DoS defenses, but concentrate on one main victim in the organization.

2.4. DoS and DDoS defense solutions

2.4.1. DoS and DDoS solutions over Application layer

- HTTP POST Flood - There is a difficulty in distinguishing between legal traffic and attack. The most effective mechanism that exists today is by combining methods of characterizing the movement of requests and identifying the source user. When a random url is used, an exception check is required to understand that this was an attack and not an innocent use of the server [3]. Part of the exception check is to try to identify the source user that triggers the attack, and you may notice that sometimes a large part of the package signature and content is the same.

- HTTPS Request Flood - Using the BIG-IP system [4] and the F5 iRules scripting language. Now available via the F5 DevCentral online community, this iRule states that if a device tries to renegotiate more than five times in any 60-second period, the connection is silently dropped. The biggest benefit to this approach is that the attacker believes the attack is still working and in service, when in actuality, the server has ignored the request and moved on to processing valid user requests instead.

- HTTP GET Flood Today We know about two detection algorithms [3], one is focusing on a browsing order of pages and the other is focusing on a correlation with browsing time to page information size. that implement detection techniques and evaluate attack detection rates, i.e., false positive and false negative. The results show that our techniques can detect the HTTP-GET flood attack effectively.

2.4.2. DoS and DDoS solutions over Transport layer

- Syn Flood - We have a lot of solution [5] for this attack: Filtering ,Increasing Backlog,Reducing SYN-RECEIVED Timer,Recycling the Oldest Half-Open TCP,SYN Cache,SYN cookies,Hybrid Approaches,Firewalls and Proxies We will expand a bit on SYN cookie is a technique used to resist SYN flood attacks. The technique's primary inventor Daniel J. Bernstein defines SYN cookies as "particular choices of initial TCP sequence numbers by TCP servers." In particular, the use of SYN cookies allows a server to avoid dropping connections when the SYN queue fills up. Instead, the server behaves as if the SYN queue had been enlarged. The server sends back the appropriate SYN+ACK response to the client but discards the SYN queue entry. If the server then receives a subsequent ACK response from the client, the server is able to reconstruct the SYN queue entry using information encoded in the TCP sequence number.

- Rst Flood - A RST packet is accepted if the sequence number is in the receiver's window, or when a connection is closed (closed socket). This is slightly different from a FIN, which just says that the other endpoint will no longer be transmitting any new data but can still receive some.

  There are three types of event that cause a RST to be emitted. A) the connection is explicitly aborted by the endpoint, e.g. the process holding the socket being killed (just closing the socket normally is not grounds for RST, even if there is still unreceived data). B) the TCP stack receiving certain kinds of invalid packets, e.g. a non-RST packet for a connection that doesn't exist or has already been closed. C) An unexpected amount of RST packets gained and there is no stopping point when sending back even a few responses. Emmiting these senarios would mitigate the performance and engagement of the server with unwanted traffic. [6].

2.4.3. DoS and DDoS solutions over Network layer

- ICMP Flood - Reconfiguring your perimeter firewall to disallow pings will block attacks originating from outside your network, albeit not internal attacks [7]. Still, the blanket blocking of ping requests can have unintended consequences, including the inability to diagnose server issues. The Incapsula DDoS protection provide blanket protection against ICMP floods by limiting the size of ping requests as well as the rate at which they can be accepted.

2.4.4. APDoS solution

To combat APDoS, organizations require a single vendor, hybrid cyber security solution that protects networks and applications from a wide range of attacks. Ideally, such a solution [8] includes all the different technologies needed for effective detection and mitigation, including DoS/DDoS protection, behavioral analysis, Intrusion Prevention System (IPS), encrypted attack protection and web application firewall (WAF). Additionally, organizations also require new levels of partnership with their DDoS mitigation service provider and any Internet Service Providerl (ISP) that provides managed DDoS services to coordinate for the effective detection and mitigation of a multi-vector assault.

3. Related Work

3.1. Related Articles

3.1.1. Traffic flooding attack detection with SNMP MIB using SVM

DoS and DDoS attacks have become more and more destructive, and are threatening to various network services. Hence, the various methods of protection and monitoring and control of network traffic have also begun. However, most of the current modern detection systems are focusing on detail analysing for each packet's data, which causes late detection and can't handle high network traffic.
Simple Network Management Protocol (SNMP)[9] provides a universal method of exchanging data for purposes of monitoring systems that reside on a network. The use of SNMP is most dominant in the modern industry. But, to utilize SNMP for traffic flooding attack detection, we need to consider the following three points in the use of the SNMP MIB variables which affects the performance and accuracy of the detection system:

- Proper selection of SNMP MIB variables for attack detection
- Determination of the detection timing about when and how often
- Algorithm for attack detection using the selected MIB (Management Information Base) variables.

3.1.2. Change trend of averaged Hurst parameter of traffic under DDoS flood attacks

DoS and DDoS flood attacks are great threats to the internet though various approaches and systems have been proposed. Hence, Intrusion Detecting System (IDS) and Intrusion Preventing System (IPS) are desired. The DDoS flood attack sends packets upon a server with a huge amount of traffic. It never tries to break into the server's system, which makes the servers's security defenses irrelevant.
The solutions given by misuse detection are primarily based on a library of known signatures to match against network traffic . Hence, unknown signatures from new variants of an attack mean are hard to be recognized. Therefore, anomaly detectors (exceeded routine detectors) play a role in detection of DDoS flood attacks.
It is important considering the Hurst parameter - H in characterizing exceptions of traffic series in packet size under DDOS flood attacks. This paper specifically [10] studies how H of traffic is changing under DDoS flood attacks. It it important understanding the following:

1. Whether H of traffic when a server is under DDoS flood attacks is much different from the regular one?
2. How is H changes when a server suffers from DDoS flood attacks?

Answering these questions might give us better understanding for detecting and protecting from DDoS flood attacks.

3.1.3. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments

Cloud computing develops rapidly due to its essential characteristics. Cloud computing would not be possible without the underneath support of networking. Recently, Software-Defined Networking (SDN) [11] has attracted great interests as a new paradigm in networking. In SDN , network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications. Denial of Service (DoS) attacks and Distributed Denial of Service(DDoS) flooding attacks are the main methods to destroy availability of cloud computing. Although the capabilities of SDN make it easy to detect and to reactDDoS attacks in cloud environments, the separation of the control plane from the data plane in SDN introduces new attack planes. SDN itself may be a target of some attacks, and potential DDoS vulnerabilities exist across SDN platforms. For example, an attacker can take advantages of the characteristics of SDN to launch DDoS attacks against the control layer, infrastructure layer plane and application layer of SDN .

3.2. Related Productions

3.2.1. Cisco - 'DDoS Mitigation'

Cisco had developed a System which delivers a complete DDoS protection solution based on the principles of detection, diversion, verification, and forwarding to help ensure total protection[12]. The solution maintains the business continuity by:

- Detecting the DDoS attack.
- Diverting the data traffic destined for the target device to a Cisco appliance for treatment.
- Analyzing and filtering the bad traffic flows from the good traffic flows packets, preventing malicious traffic from impacting performance while allowing legitimate transactions to complete.
- Forwarding the good traffic to maintain business continuity.

3.2.2. Check Point - 'DDoS Protector'

Check Point had developed a System called 'DDoS Protector'[13], which keeps businesses running with multi-layered, customizable protections and up to 40Gbps performance that automatically defends against network flood and application layer attacks with fast response time against today's sophisticated denial of service attacks.
DDoS Protector Appliances offer flexible deployment options to easily protect any size business, and integrated security management for real-time traffic analysis and threat management intelligence for advanced protection againstDDoS attacks. The product provides multi-layer protections, handles network and traffic flood and has a management system.

Acronyms

APDoS The advanced persistent denial-of-servicel. 6, 8

CDN Content delivery network. 2

DDoS distributed denial-of-service attack. 2–6, 8–10

DoS Denial-of-service attack. 2–4, 6, 8–10

ICMP Internet Control Message Protocol. 5, 6, 8

IP Internet Protocol. 2

IPS Intrusion Prevention System. 8, 9

ISP Internet Service Providerl. 8

MAC Media Access Control. 6

OSI Open Systems Interconnection. 4

SDN Software-Defined Networking. 10

SNMP Simple Network Management Protocol. 9

SSL Secure Sockets Layer. 4, 5

TCP Transmission Control Protocol. 5, 7

UDP User Datagram Protocol. 5

References

[1] Stephanie Weagle. *New Report Points to Alarming DDoS Attack Statistics and Projections*. URL: https://www.corero.com/blog/736-new-report-points-to-alarming-ddos-attack-statistics-and-projections.html.

[2] US-CERT. *DDoS Quick Guide*. URL: https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf.

[3] GENERAL SECURITY. *Layer 7 DDoS attacks: detection and mitigation*. URL: http://resources.infosecinstitute.com/layer-7-ddos-attacks-detection-mitigation/#gref.

[4] D Holmes. *Mitigating ddos attacks with f5 technology*. URL: http://nl.security.westcon.com/documents/47064/mitigating-ddos-attacks-tech-brief.pdf.

[5] Livio Ricciulli, Patrick Lincoln, and Panka j Kakkar. *TCP SYN Flooding Defense*. URL: http://ai2-s2-pdfs.s3.amazonaws.com/51f2/6c450b44ee8c5ec15945b855e34b863328f4.pdf.

[6] Juho Snellman. *The many ways of handling TCP RST packets*. URL: https://www.snellman.net/blog/archive/2016-02-01-tcp-rst.

[7] CLOUDFLARE. *Ping (ICMP) Flood DDoS Attack*. URL: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack.

[8] radware. *A Clear and Emerging Cyber-Security Threat: APDoS*. URL: https://security.radware.com/ddos-knowledge-center/ddos-attack-types/apdos-emerging-cyber-threat.

[9] Jaehak Yu, Hansung Lee, and and Daihee Park Myung-Sup Kim. "Traffic flooding attack detection with SNMP MIB using SVM". In: *Computer Communications* 31.17 (2008), pp. 4212–4219. DOI: https://doi.org/10.1016/j.comcom.2008.09.018.

[10] Ming Li. "Change trend of averaged Hurst parameter of traffic under DDOS flood attacks". In: *Computers and Security* 25.3 (2006), pp. 213–220. DOI: https://doi.org/10.1016/j.cose.2005.11.007.

[11] Qian Yan et al. "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges". In: *Communications Surveys and Tutorials* 18.1 (2016), pp. 602–622. DOI: https://doi.org/10.1109/COMST.2015.2487361.

[12] Cisco System. *Defeating DDos attacks*. URL: https://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.pdf.

[13] Cheack Point. *DDoS protector appliance*. URL: https://www.checkpoint.com/downloads/product-related/datasheets/ds-ddos-protector-appliances.pdf.