A Solution for the Security Attack Using Distributed Denial of Services

Ivan Georgiev[1] and Kamelia Nikolova[2]
Faculty of Telecommunications at Technical University of Sofia
8 Kl. Ohridski Blvd
Sofia 1000, Bulgaria
{ivanegeorgiev@tu-sofia.bg, ksi@tu-sofia.bg}

ABSTRACT: *Distributed Denial of Service is a normal type of security attack for which network protection is deployed. Network resources are aimed by this attack which is now studied. We have used a solution named as DenfensePro for safeguarding the network resources. We have tested the efficiency of the introduced solution for network resources protection.*

Keywords: Distributed Denial of Service, Attacks, Network Resources, Data Center

Received: 29 January 2020, Revised 18 March 2020, Accepted 12 April 2020

DOI: 10.6025/isej/2020/7/1/9-15

1. Introduction

Since the first denial of service (DoS) attack in 1974, Distributed DoS (DDoS) attacks have remained among the most significant and damaging cyber attacks. They receive much attention in last two decades [1]-[9] and play an important role when designing network topology. Both DoS and DDoS attacks are a major threat to the operation of websites, applications and servers, but the problem of DDoS is more complex and difficult to be solved due to two main reasons [6]. Firstly, DDoS attack uses more than one network node and more than one network connectivity thus each victim regardless as well be secured can become inactive. Secondly, the use of seemingly legitimate traffic complicates the response because it is difficult to identify and block the attack without compromising the legitimate users.

The problem with DDoS attacks is even more relevant in data centers where multiple organizations host their servers providing different functions and services. As data centers are the most popular location for Software Defined Networks / Network Functions Virtualization (SDN/NFV), proper planning of the network and the use of specialized hardware/software to prevent DDoS attacks are required [3][7][8]. Building a working system to stop malicious attacks includes not only its design but also an analysis of the functionality and effectiveness [5]. A number of possible approaches to implement network protection are proposed and described in the literature [1]-[9]. More than a hundred of publications on DDoS attacks and defense approaches published in last fifteen years are reviewed and discussed in [1][2]. A conceptual framework was also presented in [1], where

change point detection of packet inter-arrival time was used to detect different forms of DDoS attack in the cloud. A broad classification of various DDoS attacks, DDoS defensive architectures, such as source-end, victim-end and intermediate architectures, as well as various detection and mitigation mechanisms such as statistical based, soft-computing based, knowledge based and data mining based approaches are presented and analysed in [2].

In real time networks, it is not possible to fulfil all the requirements for DDoS detection and various performance parameters must be taken into account and need to be carefully balanced against each other. Thus, there is no universal solution how to protect and secure the network.

The main aim of this paper is to propose an approach to protect a Data Center Network against DDoS attacks targeting network resources. After a carefully analysis of the possible solutions, a hardware firewall is selected and configured. Some experiments are conducted, verifying the performance of the applied solution.

This paper is organized into 6 sections. In Section II the different types of DDoS attacks targeting network resources are considered. Possible software and hardware solutions to prevent network resources against DDoS attacks, together with their position in the network topology are analysed in Section III. An approach of network protection is proposed in Section IV, while the conducted experiments and analysis are given in Section V. Concluding remarks are presented in Section VI.

2. Types of DDOS Attacks Targeting Network Resources

There exist a number of classification of various DDoS attacks in [2][5][6]. They can be classified by [2] attack rate (continuous, or variable rate), by impact on service availability (disruptive, or degrading the services) and by exploited vulnerability through which an attacker launches attack on the victim (bandwidth, or resource depletion).

Attacks targeting network resources aim to deplete the entire victim's bandwidth by using a large amount of illegitimate traffic. This type of attacks, often called "network flood" is very simple to be implemented. They can be realized as UDP (User Datagram Protocol) flood, ICMP (Internet Control Message Protocol) flood, IGMP (Internet Group Management Protocol) flood, amplification attacks, connection-oriented attacks, connectionless attacks and reflective attacks [6]. The UDP flood attack is based on sending a large amount of UDP datagrams from potentially falsified IP (Internet protocol) addresses to random server-victim's port [8]. The server receiving this traffic tries to find application that listen on this port and to respond with ICMP Destination Unreachable message in case of no such application. Thus, the server becomes enable to process every request due to bandwidth consuming. UDP flood considered as a volumetric attack is measured in Mbps (bandwidth) and PPS (packets per second). The ICMP flood attack is also a volumetric attack [6] which can use every ICMP message type (ping request is commonly used). Once enough ICMP traffic is sent to a target server, the server becomes overwhelmed from attempting to process every request, resulting in a denial-of-service. The operating principle of IGMP flood attack [6] is similar to above mentioned attacks, but includes a large number of IGMP messages resulting in denial-of-service conditions. The amplification attack uses the discrepancy between requests and responses in communication. Smurf attacks (ICMP amplification) and Fraggle attacks (UDP amplification) are typical representatives, as well as DNS amplification.

The connection-oriented attack requires to establish a connection prior to initiate DDoS attacks. As a result the server and application resources are depleted. TCP (Transmission Control Protocol)- or HTTP (Hypertext Transfer Protocol)-based attacks are typical examples. TCP SYN flood attack is the most popular one. Although the connectionless attacks (for example UDP floods and ICMP floods) does not require to establish a connection they affect network resources causing denial of service before the malicious packets can even reach the server. The attack can be classify as reflective when the attacker makes use of a potentially legitimate third party to send his or her attack traffic, ultimately concealing his or her own identity [6].

3. Protection Methods Against DDOS Attacks

DDoS attacks are even more devastating in data centers. Considering the fact that in these facilities various type of equipment is collocated, providing a number of different services, DDoS attacks are frequent issues. All types of attacks, described above, could be observed at the data center's network, and they vary in target, volume and duration. The no-volume-

tric ones affect only the targeted IP address or service. The incoming traffic of massive DDoS attacks, however, physically overloads the links from the Internet to the international routers of the data center. This is the worst case scenario, because the targeted client as well as the other customers begin suffering packet loss. In this case, the issue must be immediately addressed by network administrators in order to stop the traffic and disengage the international bandwidth.

Considering current network design, the following actions could be performed:

• **Access control list (ACL) filtration** - ACL is a way to affect the malicious traffic by traffic inspection based on predefined rules. Nevertheless the various functions for traffic filtering, based on direction, IP addresses, TCP/UDP transport and ports, ACLs could be more appropriate for DoS, rather than DDoS attacks. The network devices' filtration principle is based on packet processing according to the configured ACLs. This function is done by the device central processing unit (CPU) and if attack with volume of several Gb/s has to be processed, this may cause CPU overload and even device failure. This is the reason, ACLs not to be used for defense mechanism against DDoS.

• **Blackhole (null-route) -** The blackhole function is another way of dealing with malicious traffic. It's just a routing table entry, which is propagated to the Internet Service Provider (ISP), in this way instructing their router to send the traffic towards "null-route" or in other words - to drop it. Because it's simple and effective, this is the way to stop ingress volumetric DDoS attacks. In this way, the malicious traffic do not reach the data center's network and do not cause international links overflow. And yet, this method has its disadvantages – null-route creation stops all the incoming traffic towards the attacked IP address. Even if there is legitimate traffics towards the victim IP address, it would be discarded and again denial of service is caused.

By the analysis made so far regarding the network design and ways of dealing with DDoS, it turns out that services offered by data centers need dedicated system for protection against such threats. DefensePro [10], a Radware product, is an Intrusion Prevention System (IPS) device for defense against DDoS attacks, which provides business continuity of ISPs by dealing with present and emerging network-based attacks. The system inspects in real time the incoming traffic for potential threats and if such is detected it gets discarded. Choosing this device is based on the fact that despite the traditional IPS systems, DefensePro has the ability of detecting network and system resources abuse, malware spread, authentication intrusion and identity theft [10]. The existing features, providing full protection against traditional vulnerability-based attacks, known worms, trojans, bots and SSL-based attacks make it exclusively suitable for DDoS mitigation. Furthermore, behaviour-based, automatically generated in real-time signatures allow "zero-minute" attack detection such as: network and application flood, HTTP flood, malware, website hacking, brute force attacks, etc. DefensePro system consists of the following components [10]:

• **DefensePro device –** The term device refers to the physical platform, used for traffic filtration; · Management interface – APSolute Vision – physical device, which provides functions for configuration, monitoring and reporting;

• **Ràdwàre security update service –** Web platform providing periodic or emergency signature updates. In this way, the system can address new-come security threats such as worms, trojans, bots and application vulnerabilities. There are two ways to implement the IPS in a production network [10]:

• **Typical deployment -** As a transparent device for entire international traffic. DefensePro is placed between data center's ISP and the international routers, in this way protecting all the devices behind it against ingress attacks.

• **Out-of-path deployment -** As a device deployed outof-path for the incoming traffic, which also provides full mitigation capabilities. In this way the IP ranges that should be protected against DDoS are routed through the device, where the traffic is cleansed and returned back to the core network. For this contribution out-of-path deployment is chosen, due to the following reasons:

• The typical deployment is more suitable for newnetwork design. As the data center's network is in production, deploying new device in this way would cause service interruption for the customers. Furthermore, if DefensePro is a device used for the first time, the initial testing is needed before routing customer's traffic through it.

• Despite the various features for DDoS mitigation, technological time is needed for the system to start detecting malicious

traffic. A separate network class (set of rules and policies for traffic inspection) for each customer must be configured. That means it's impossible to migrate at once all incoming traffic to the data center's network.

• Another consideration, that suggests this deployment is the fact that data center's network except four links to the Internet, also has a number of regional peering links. These connections exceed the number of physical interfaces of the DefensePro. Last but not least, hardware and software firewalls are considerably expensive tools for attack mitigation. Thus, DDoS mitigation system will be offered as a separate service and only the traffic of these, who requested protection should be routed through it.

4. Network Topology

Network topology of the data center considered in this contribution is shown on Figure 1 and is consisted of the following devices:

- International routers - INT1/INT2 - used for international connectivity only and for limiting the bandwidth according to the negotiated capacity for every customer.

- Core routers - CORE1/CORE2 - used for customer traffic diversion between international and regional destination.

- Access switches – provide physical connectivity with Customer1 (for short called C1)

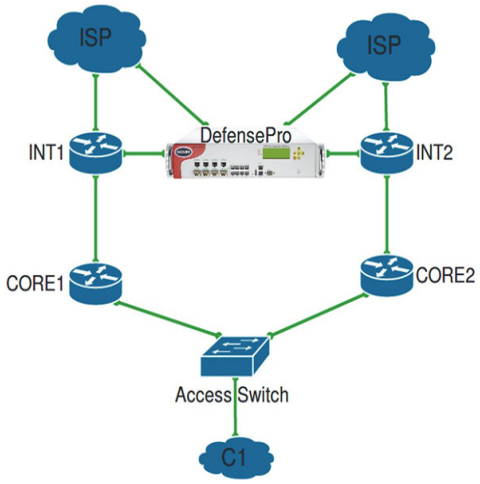

Figure 1. Physical Network topology

DDoS attacks towards C1 have two possible routes:

• INT1 → CORE1 → Access Switch → C1;

• INT2 → CORE2 → Access Switch → C1.

Components of logical network topology for DefensePro deployment are given in Fig. 2. The blue line represents normal traffic, the red one – "dirty" traffic, while the green one – "cleansed" traffic to the destination.

• Bypass switch – active hardware device used for eliminating service interruptions during failures or device maintenance;

• Aggregation switch – used for traffic aggregation from different Virtual Local Area Networks (VLANs) and sending it to the Bypass by means of trunk ports;

• Customer router – Provides routing of cleansed traffic towards customers

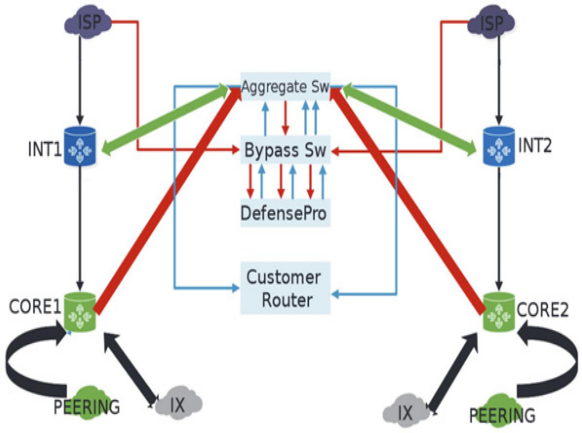

Figure 1. Logical Network topology

A customer C1 who requires DDoS protection for its network infrastructure is considered in this paper. For the purposes of the study, a network-based class is applied, thus all IP addresses used by C1 are grouped in one network class. In order to implement DDoS flood protection a behavioral DoS (BDoS) profile for C1 is configured. This protection type can be adjusted according to the protected capacity and expected traffic. Typical for the behavioral protection is that there is no training and always must take into account the parameters specified by the administrator. The following different types of DDoS flood protections are included in C1 BDoS profile: TCP, UDP, ICMP and IGMP.

The bandwidth and quota settings [10] must also be set carefully because they affect directly the sensitivity of attacks detection. The bandwidth capacity for C1 which is considered in this paper is 100 Mbit/s in both directions. Quotas include the percentage of expected maximal traffic of TCP, UDP, ICMP and IGMP to the total traffic for each transmission direction. For C1, the configured values are respectively 75%, 50%, 2% and 2%. The amount of them may exceed 100% because the values represent the maximum volume of traffic for a protocol based on the total amount of traffic. The UDP packet rate detection sensitivity is set to “low”.

The connection limit profiles configuration will prevent attacks based on sessions, such as half-open SYN attack, attack with a large number of requests and such a large number of connections. Limit connections profile includes definitions of attacks targeting groups of TCP or UDP ports. For this study, link restriction for protocols HTTP (port 80) and HTTPS (port 443) are considered for C1 and are given in Table 1.

5. Experiments

Name	TCP port 80	UDP port 80	TCP port 443	UDP port 443
Application	HTTP	HTTP	HTTPs	HTTPs
Protocol	TCP	UDP	TCP	UDP
Number of connections	100	100	100	100
Tracking type	Source Count	Source Count	Source Count	Source Count
Action Mode	Drop	Drop	Drop	Drop
Risk	Medium	Medium	Medium	Medium
Suspend Action	Source IP	Source IP	Source IP	Source IP

Table 1. Connection limit Protection For Customer 1

In order to demonstrate DefensePro functionality, a captured DDoS attack is analyzed. Traffic graph towards C1 at the begin ning of a flood attack is shown on Fig. 3. Time span is set to 1 hour and during this time interval the legitimate traffic (with blue line) does not exceed 100Mb/s. The red line indicates about 800Mb/s dropped traffic of the DDoS flood attack.

The whole attack is given on Figure 4 where it can be seen that the flood traffic reaches 8 Gb/s.

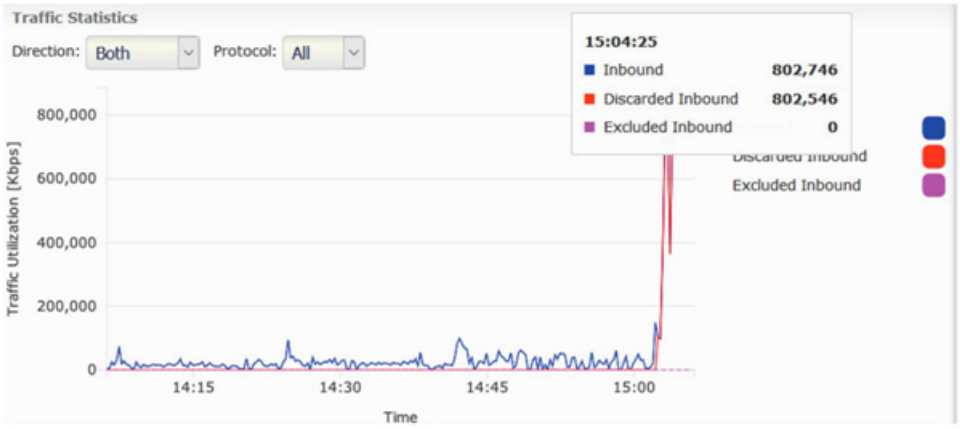

Figure 3. Input Traffic to customer1 at the beginning of the attack

Figure 4. Input traffice to customer1 during attack

Such volume of flood attack would overflow Internet capacity of C1 if there is a lack of DDoS mitigation system and would

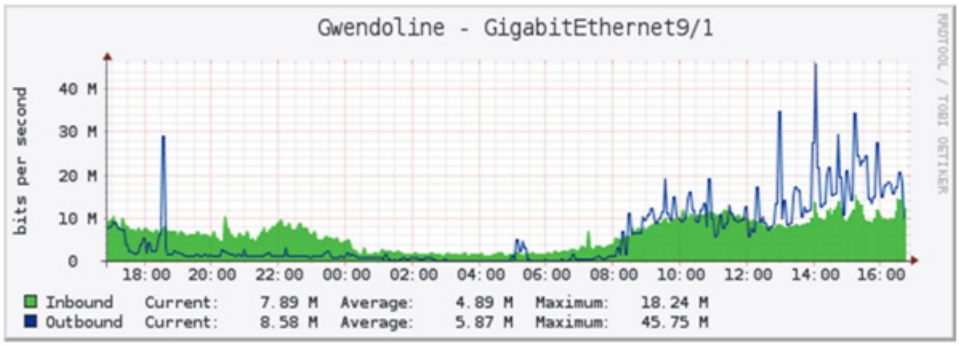

Figure 5. Traffic On customer1 physical port

cause denial-of-service condition. Furthermore, inbound volumetric traffic would cause Internet connectivity problems for most of customers of the data center. Using mitigating capabilities of DefensePro, only the malicious traffic is dropped and the legitimate one is unaffected, in this way providing business continuity. The traffic of the physical port of C1 captured by means of Cacti software [11] is given on Figure 5.

As it could be seen during the DDoS attack, only a slight traffic increase is observed (blue line), which proves that the system has successfully mitigated the DDoS attack. Detailed report on the detected DDoS attack is prepared by DefensePro system, but because of the paper limit is not given here.

6. Conclusion

An approach of network protection against DDoS flood attacks targeting network resources was proposed. An IPS DefensePro "out-of-path deployment" system was implemented and configured. Following the results obtained from experiments the main conclusion is that the proposed design is working properly and can successfully protect the network topology so considered. Keep in mind that the real time network protection has a number of aspects that must be carefully analyzed and taken into account, the ideal solution does not exist and thus the DDoS protection remains the hottest research area.

Acknowledgement

The research is conducted under the grant of project DH07/10-2016, funded by National Science Fund, Ministry of Education and Science, Bulgaria.

References

[1] Osanaiye, O., Choo, K.R., Dlodlo, M. (2016). Distributed Denial of Service (DDoS) Resilience in Cloud: Review and Conceptual Cloud DDoS Mitigation Framework, *Journal of Network and Computer Applications*, vol. 67, p 147-165, May 2016.

[2] Prasad, K., Reddy, A., Rao, K. (2014). DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms - A Survey, *Global Journal of Computer Science and Technology: (E) Network, Web & Security*, 14 (7), Ver. 1.0, p 15-32, 2014.

[3] Wang, B., Zheng, Y., Lou, W., Hou, Y. T. (2015). DDoS Attack Protection in the Era of Cloud Computing and Software-Defined Networking, *Computer Networks*, 81, p 308-319, 2015.

[4] Nunes, I., Schardong, F., Schaeffer-Filho, A. (2017). BDI2DoS: An Application Using Collaborating BDI Agents to Combat DDoS Attacks, *Journal of Network and Computer Applications*, vol. 84, p 14-24, 2017.

[5] Anstee, D., Bowen, P., Chui, C.F., Sockrider, G. (2017). Worldwide Infrastructure Security Report, Arbor Networks Special Report, Vol. XII, Arbor Networks, 2017. (www.arbornetworks.com)

[6] Radware, DDoS Handbook, 2015.

[7] Shameli-Sendi, A., Pourzandi, M., Fekih-Ahmed, M., Cheriet, M. (2015). Taxonomy of Distributed Denial of Service Mitigation Approaches for Cloud Computing, *Journal of Network and Computer Applications*, vol. 58, p 165-179, 2015.

[8] Dzurenda, P., Martinasek, Z., Malina, L. (2015). Network Protection Against DDoS Attacks, *Intern. Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, 4 (1), p 8-14, 2015.

[9] Zhou, W., Jia, W., Wen, S., Xiang, Y., Zhou, W. (2014). Detection and Defense of Application-Layer DDoS Attacks in Backbone Web Traffic, *Future Generation Computer Systems*, vol. 38, p 36-46, 2014.

[10] Radware, DefensePro User Guide, January 2016.

[11] Berry, I., Roman, T., Adams, L., Pasnak, J.P., Conner, J., Scheck, R.. Braun, A. (2017). The Cacti Manual, The Cacti Group, 2017.