DPNI: A FRAMEWORK FOR QUANTIFYING DDOS ATTACK IMPACTS ON VARIOUS WEBSITES

N.Srihari Rao[1], K.Munidhanalakshmi[2], Y.Sirisha[3], B.Ajay Kumar[4], and B.Chandra Lekha[5]

[1,2,3]Assistant Professor, CSE Department, BIET Hyderabad, Telangana, India
[4]Student, ECE Department, BIET Hyderabad, Telangana, India
[5]Student, CSE Department, BIET Hyderabad, Telangana, India.

Abstract: Internet is built for providing huge resources to its users and positively sharing the available resources among its users. It is not built with security in mind in the beginning and hence opened doors for many kinds of abuse by malicious users. Any website with few or many web pages can be DDoSed to disable the web servers from serving legitimate users. Interestingly, some web servers are almost unaffected or affected but not manifested through these attacks, therefore these kinds of websites need not plan for and deploy DDoS protection mechanisms in reality. When the attackers' attempts do not affect the good intended outcomes, the problem can be considered to be trivial. We devised a framework namely "DDoS Protection Necessity Index (DPNI)" for evaluating the need of DDoS defense for different categories of websites on the Internet. This framework is deemed to be reliable and effective.

Keywords: Internet, Distributed Denial-of-Service(DDoS) Attacks, Flash Crowds (FCs), Load Testing, Hyper Text Transfer Protocol (HTTP), Attack Impact, DDoS Protection Vendors (DPVs).

I. INTRODUCTION

There exist different types of websites driven with different motivations [1]. Some websites may target for making money, gaining popularity, personal satisfaction, or malicious purposes [2]. We need some common criteria that can be utilized to determine the need of the DDoS protection service for any website [3]. DDoS protection becomes a necessity, if the website that serves the users faces the DDoS attacks and owner of the website feels and imagines the negative impact on his website in certain definable terms. Therefore, there must be some mechanism to assess and quantify the DDoS attack impact on any website and evaluate the need for DDoS defense for that website in the presence of potential victims (persons). Currently, in the DDoS defense industry there are many DPVs [4,5] each of which has different mechanisms to back website owners and support 24/7 availability of web servers to its users.

The paper is organized as follows. Section II presents the literature review of the existing methods deployed by the DPVs to provide DDoS protection services. Section III presents the parametric analysis of the impact of DDoS attacks on a variety of websites. Section IV demonstrates the performance test for any web server under consideration. Section V concludes the paper and presents the future scope for this work.

II. RELATED WORK

Akamai's DDoS mitigation solution[4,5] can include Content Distribution Network (CDN)-based, DDoS scrubbing, and/or DNS components, depending on each customer's requirements. DDoS protection is priced based on a consultative approach to identifying the customer requirements, including 1.Assets being protected, 2.Scale of assets being protected, 3.Deployment model 4.Service model selected, and 5.Additional options selected. Verisign, a DDoS Protection Service vendor offers monitoring and on-demand mitigation capabilities. When the company's monitors detect a DDoS attack, support personnel notify the customer about the attack and recommend a mitigation strategy. If a third-party monitoring service is being used or if a company monitors its own network, the customer can notify Verisign when to begin mitigation. Verisign also offers the OpenHybrid API, which allows

organizations to use their existing security devices to send threat information to Verisign's cloud-based solution. Verisign does not disclose its pricing strategy.

Radware's suite of DDoS protection solutions and web application security offerings provide integrated application and network security solutions. Its Attack Mitigation Solution (AMS) is a hybrid DDoS protection solution that integrates always-on detection and mitigation (on-premises or in the cloud) with cloud-based volumetric DDoS attack prevention, scrubbing, and 24x7 cyber attack and DDoS security. Radware does not disclose its pricing strategy. Cloudflare has an always on, cloud-based DDoS protection system. Instead of using dedicated anti-DDoS hardware, every single machine in its global network takes part in DDoS mitigation. With over 15 Tbps of capacity, it can scale up to handle the biggest DDoS attacks. It has different plans for different requirements. It serves Free tier $0/month; Pro $20/month; Business $200/month and Enterprise pricing on request.

Arbor Availability Protection System (APS) [6]: Arbor utilizes hybrid, multi-layer defense to protect against all types of DDoS threats. This includes cloud-based protection to defend against large, high-volume attacks. On-premises protection also protects against complicated application-layer and TCP state-exhaustion attacks. Arbor APS incorporates detection and mitigation technology, providing a view of network activities and enabling fast, automatic blocking of attacks before those impact critical applications and services. Arbor does not disclose its pricing strategy. Nexusguard's solution mitigates all types of DDoS attacks and cyber threats, delivering maximum uptime to organizations with an online presence. This encompasses protection against level 3 to level 7 attacks including DDoS attacks, TCP SYN+ACK, TCP FIN, TCP RESET, TCP ACK, TCP PSH+ACK, TCP fragment, UDP, Slowloris, spoofing, ICMP, IGMP, HTTP flood, brute force, connection flood, ping of death, Smurf, reflected ICMP and UDP, SSL flood, zero-day attacks and more. Nexusguard does not disclose its pricing strategy.

DOSarrest is focused on HTTP/HTTPs and protecting websites, APIs and mobile application servers on TCP ports 80 and 443. It offers a fully managed cloud-based security solution, made up of DDoS protection, a web application firewall, a CDN for enhanced performance, website monitoring and support. All are integrated using its big data analytics engine. It also monitors websites outside its own network from 10 different locations around the globe. Additionally, it offers cloud-based global and local load balancing. DOSarrest offers two fully managed plans starting from $700/month. F5 Networks DDoS Protection takes a four-tier approach to protecting against DDoS traffic: cloud, network, application and DNS. It can examine network layers 3-7. F5's DDoS Hybrid Defender provides multi-layered defense that protects against blended network attacks and sophisticated application attacks while enabling full SSL decryption, anti-bot capabilities and advanced detection methods in one appliance. F5 Networks does not disclose pricing.

Neustar SiteProtect NG offers both on-premises and cloud options. With 4 Tbps of capacity, its cloud-based DDoS protection service scrubs malicious traffic to defuse large and complex attacks. It can put countermeasures in place to limit exposure, protect a site's uptime and preserve a brand's reputation. Neustar provides automated mitigation across multiple attack vectors. It recently launched an integrated Web application firewall (WAF) solution that works in tandem with its cloud DDoS mitigation. Neustar offers pricing based on the level of risk rather than the traditional pay-per attack. Imperva Incapsula like other vendors uses a multi-tier approach to blocking DDoS traffic. Imperva Incapsula filters traffic through a web application firewall, a DDoS rules engine, and a series of progressive challenges. The process is said to be invisible to legitimate traffic, and legitimate visitors will not encounter latency, CAPTCHAs or wait screens. Its business plan sells for $299 per site per month and Professional plans sell for $59 per site per month.

N.S.Rao et. al. carried out the research work [1] for a clean classification of all websites for considering the DDoS attack impacts on these websites. Their work also presented detailed benefits and beneficiary categories for different types of websites. Currently, standard evaluation procedure or mechanism does not exist for determining the degree of necessity for DDoS protection. Hence, we have taken up the task of devising a framework with a set of standard evaluation criteria for determining the degree of DDoS defense necessity. We designated the framework with necessary mechanisms for this evaluation as "DDoS Protection Necessity Index (DPNI)".

III. Parametric Analysis of the Impact of DDoS Attacks on Different Websites

DDoS Protection Vendor (DPV) companies offer DDoS Protection plans for customer's websites. DPVs generally prepare a quotation for a particular DDoS Protection plan based on some important elements that the customers seek from these vendors. For example, Cloudflare company [7,8] offers "Pro" plan for professional web sites, "Business" plan for small enterprise websites, and "Enterprise" plan for companies requiring enterprise-grade security and performance. The cost of these DDoS Protection plans varies from plan to plan. It is important for DPVs to be accurate in assigning a particular protection plan to customers in order to develop and maintain continuous good business relationships with the customers who seek DDoS Protection plans.

3.1. Proposed Evaluation Criterion

As an initiative to take up the DDoS defense, in the requirements gathering phase from customers, DDoS attack analyst may enquire about two kinds of factors namely 1. Concrete Factors (these factors can be accurately assessed from site's performance and experience and are generally specific to the customer's website) and 2. Human Willingness to have DDoS Protection factors (these factors depend upon the customer's mindset and his willingness to subscribe for DDoS protection plan). In the context of any website, we can use a common formula in order to determine the degree of necessity of DDoS protection plan which we designate as DDoS Protection Necessity Index (DPNI). The DPNI value is calculated using the following formula. DDoS Protection Necessity Index (DPNI) = Weight from Concrete Factors (WCF) + Weight from Human Willingness to have DDoS Protection Factors (WHWF).

A. Weight from Concrete Factors (WCF)

Weight from Concrete Factors (WCF) is calculated using the Concrete Factors that include the following:

i) Sensitivity to Financial Impact (SFI): Describes the level of sensitivity for monetary gains or pains from its website services. SFI = A1, where 1<=A1<=10.

ii) Impact from Seasonal Effects (ISE): Describes the level of sensitivity for different seasons of its website service's business. ISE = A2, where 1<=A2<=10.

iii) Popularity Index (PI): Describes the level of sensitivity for its popularity or de-popularity. PI = A3, where 1<=A3<=10.

iv) Future Potential for the website (FPW): Describes the level of sensitivity for its future and its potential business in future. FPW = A4, where 1<=A4<=10.

v) Regular Hike in the Client Base (RHCB): Describes the level of sensitivity for the regular hike or fall in client number for its website services. RHCB = A5, where 1<=A5<=10.

vi) Income Sources from Users of Client's Website (ISUCW): Describes the level of sensitivity for its income sources from the users of its client's website services. ISUCW = A6, where 1<=A6<=10.

vii) Impact from Special Events (ISPE): Describes the level of sensitivity for some special events to its website's services such as Flash Crowd event. ISPE = A7, where 1<=A7<=10.

viii) Desired Network uptime Level (DNUTL): Describes the level of sensitivity for network uptime or downtime levels. DNUTL =A8, where 1<=A8<=10.

Weight from Concrete Factors (WCF) = (SFI + ISE + PI + FPW + RHCB + ISUCW + ISPE + DNUTL)/8

B. Weight from Human-Willingness to have DDoS Protection Factor (WHWF)

Weight from Human-Willingness to have DDoS Protection Factor (WHWF) is calculated using the Human-Willingness to have DDoS Protection Factors that include the following:

i) Score for Detection Wanted (SDW): Describes the score given by the client for its want for DDoS detection. SDW = B1, where 1<=B1<=10.

ii) Score for Protection Wanted (SPW): Describes the score given by the client for its want for DDoS protection. SPW = B2, where 1<=B2<=10.

iii) User's Satisfaction Level (USL): Describes the score given by the client for its want for level of its users' satisfaction. USL = B3, where 1<=B3<=10.

iv) Vulnerability Index as Assessed by Client (VIAC): Describes the score given by the client for the vulnerability degree of its web server. VIAC = B4, where 1<=B4<=10.

Weight from Human Willingness to have DDoS Protection Factor (WHWF)= (SDW + SPW + USL + VIAC)/4

Now DPNI is calculated by adding WCF and WHWF. DPNI= (WCF+WHWF)/2. Based on their previous experiences, the DPVs can judge the customer's applications for subscribing to DDoS Protection using the DPNI obtained using the above mentioned calculations. Generally, if the DPNI value is above 5, then the DPVs may immediately confirm the formal and official applications of customers to subscribe for DDoS Protection plans. Otherwise the customers may be asked to undergo some delay by waiting before availing DDoS Protection plans.

3.2. Illustration of the working of DPNI framework for an Example Website [9]

(https://sites.google.com/site/nsrihariraophd/)

Factors (Under 2 Categories)	Client-Filled-in Values	Threshold Values	Remarks	Average Value
1. WCF				
SFI	6	5		49/8= 6.125
ISE	5	5		
PI	8	5		
FPW	7	5		
RHCB	5	5		
ISUCW	6	5		
ISPE	7	5		

DNUTL	7	5		
2. WHWF				
SDW	7	5		29/4= 7.25
SPW	8	5		
USL	7	5		
VIAC	7	5		
			DPNI Value	6.69
Final Decision: DDoS Protection is suggested for the given website as calculated DPNI value is 6.69 which is far above 5.				

IV. DoSHTTP Tool Useful as a Load Tester

The performance test for a website can be used for quantifying the client base that can be supported by the web server. When the client base is quantified, it can be used for understanding the impacts of DDoS attacks or Flash Crowds (FCs) [10,11,12] on a website. If the quantification of client base is correlated with the anomalous conditions may it be either DDoS attack or FC traffic conditions, precautionary and novel preventive approaches against damage can be invented and deployed for an effective DDoS protection.

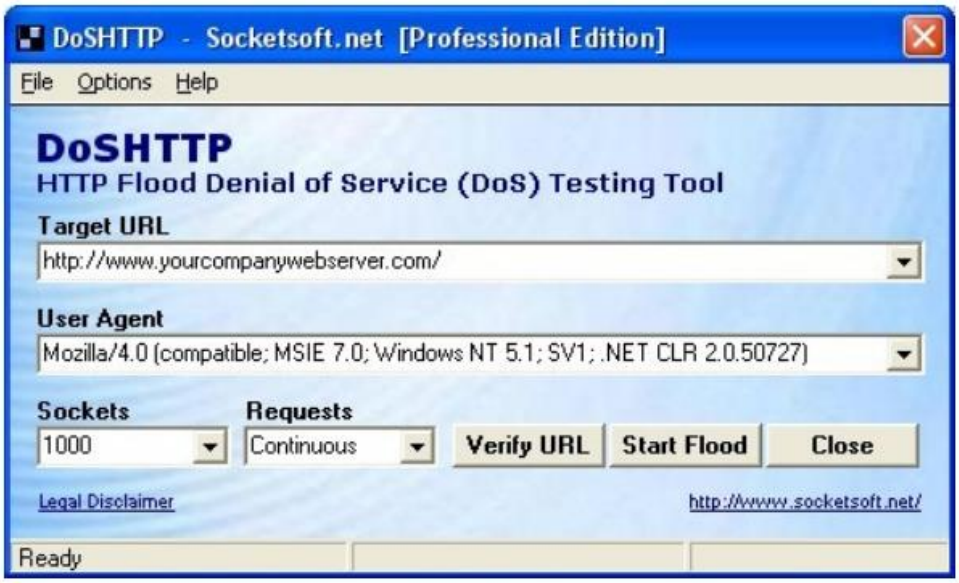

Figure 1. Screenshot of the DoSHTTP Tool working as a Load/Performance Tester

We have used DoSHTTP tool as a HTTP Flood Denial of Service (DoS) testing tool to test the web server (http://www.yourcompanywebserver.com) against the load (which means the maximum number of requests that can be served by the web server at a certain point of time) as the screenshot in figure 1 shows. Table 1 presents different performance test cases for different number of connections for the DoSHTTP tool.

Table 1. Performance Test Cases for the DoSHTTP Tool

S.No.	Test Case	No. of Connections	Test Passed (Yes/No)?
1	TC1	1000	Yes
2	TC2	2000	Yes
3	TC3	3000	No

V. Conclusions and Future Scope

We perceived that not all web servers are equally affected or damaged [2] through DDoS attacks as some web servers are almost unaffected or affected but not manifested through these attacks. Therefore, these kinds of websites need not plan for and deploy DDoS protection mechanisms in reality. We needed to have a framework for determining the degree of the necessity of DDoS protection service for different categories of websites. We proposed a framework named "DPNI" for enabling DPVs to work as an intelligent recommender for the clients, who look for or approach for DDoS Protection plans. DPNI framework is deemed to be a reliable and effective way for evaluating the real need of DDoS protection for a particular customer's website. As part of our future work we would like to test this DPNI framework over a reasonable number of DDoS Protection clients and their counterparts to verify the superiority of this framework.

VI. Acknowledgements

We would like to thank BIET college management for the valuable support, and Prof.K.Chandra Sekharaih, Research Advisor, JNTUH for his guidance in writing this research paper.

References

[1] J.Ramesh Babu, K.Chandra Sekharaiah, N.Srihari Rao. (2017) "Adaptive Management of Cybercriminal, Maladaptive Organizations, in the Offing, that Imperil the Nation." in Tech-Report-JNTUH-CHANDRG-RB-NSRAO-1.

[2] N.Srihari Rao, K.Munidhanalakshmi, Y.Sirisha, V.Shashidhar Reddy, and T.Geetha Sri, "Classifying Websites for Quantifying DDoS Attack Impacts", in Tech-Report-BIET-NSRAO-KMDLAKSHMI-YSIRISHA-1.

[3] Website, From Wikipedia, the free encyclopedia, URL: https://en.wikipedia.org/wiki/Website

[4] Top 10 Distributed Denial of Service (DDoS) Protection Vendors URL: https://www.esecurityplanet. com/ products/top-ddos-vendors.html

[5] DDoS Protection Services by Business.Com Editorial Staff URL: https://www.business.com/ categories/best-ddos-protection-services/

[6] Why do you need on-premise DDoS protection? URL: https://www.arbornetworks.com/blog/insight /why-do-you-need-on-premise-ddos-protection/

[7] Cloudflare Pricing URL: http://www.Cloudflare.com/plans

[8] Protect Against DDoS Attack, URL: https://www.cloudflare.com/ddos/

[9] https://sites.google.com/site/nsrihariraophd/

[10] N.Srihari Rao, K.Chandra Sekharaiah, A.Ananda Rao, "A Survey of Discriminating Distributed DoS Attacks from Flash Crowds." in Springer Computer Science Proceedings, Communications in Computer and Information Science (CCIS) Series, Springer, Singapore, Vol.628, pp. 733-742, ISSN: 1865-0929 **and** Presented in First International Conference on Smart Trends for Information Technology and Computer Communications (SmartCom-2016), 6th -7th August 2016, Jaipur, India.

[11] N. Srihari Rao, K. Chandra Sekharaiah and A. Ananda Rao, "An Approach to Distinguish the Conditions of Flash Crowd Versus DDoS Attacks and to Remedy a Cyber Crime", International Journal of Computer Engineering and Technology (IJCET), 9(2), 2018, pp. 110-123.

[12] N.Srihari Rao, K.Chandra Sekharaiah, A.Ananda Rao. (2017) "A Survey of Distributed Denial of Service (DDoS) Defense Techniques in ISP Domains." in Proceedings of 5th International Conference on Innovations in Computer Science and Engineering (ICICSE-2017), Hyderabad, 16th-17th Aug 2017, pg.24-25, **and** in Springer Lecture Notes in Networks and Systems (LNNS) series, Vol.32, Springer, Singapore, pg.221-230, ISBN:978-981-10-8201-6 .