Performance Comparison of Defense Mechanisms Against TCP SYN Flood DDoS Attack

Samad S. Kolahi, Amro A. Alghalbi , Abdulmohsen F. Alotaibi, Saarim S. Ahmed, and Divyesh Lad
Unitec Institute of Technology, Auckland, New Zealand
skolahi@unitec.ac.nz
amro-alghalbi@live.com

Abstract –The TCP SYN DDoS attack and defense prevention mechanisms is studied. Each prevention mechanism has some exclusive pros and cons over the others. In this paper, we have compared various defence mechanisms for preventing potential TCP SYN DDoS attacks. Router based TCP Intercept is found to provide the best defense while Anti DDoS Guardian gave the worst defese.

Index Terms –DDoS, TCP SYN Flood attack, DDoS defenses

I. Introduction

Internet usage is mounting at an exponential rate as organizations, governments and citizens continue to upsurge their reliance on this technology. Unfortunately with an increase in number of host, count of attacks on Internet has also increased incredibly fast. DDoS (Distributed Denial of Service Attack) is one of the most common and major threat to the Internet in which the goal of the attacker is to consume computer resources of the victim, usually by sending a high volume of seemingly legitimate traffic requesting some services from the victim. With DDoS Attack, the attacker uses spoofed IP address so it can't be traced back and get caught. The attacker can also use other computers as Zombies to attack the victim.

Same Types of DDoS attacks are TCP SYN Flood, Smurf attack and IPV6 RA (Router advertisement) attack, and UDP Attack. The Smurf Attack is an attack in which numerous ICMP (Internet Control Message Protocol) packets with the envisioned victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. This causes all hosts on the network to reply to the ICMP request, causing significant traffic to the victim's computer. In an IPv6 RA attack, the attacker floods the network with a large number of rough IPv6 RA packets, from different sources. These packages usually look like genuine packets from the router but they contain fake information. In UDP Attack, The attacker can send a large number of UDP packets to random ports on a remote host.

A TCP SYN flood is a form of denial of service attack in which an attacker sends many SYN requests to a target's system in an attempt to consume sufficient server resources and network bandwidth to make the system impassive to legitimate traffic [1]. TCP SYN flood attack exploits the generic design of the TCP protocol. Any TCP based application it is required to complete the TCP 3 way handshake, before the data transfer. TCP SYN Flood attack is investigated in this paper. TCP SYN Flooding has remained one of the most destructive attack since September 1996; numerous sites on the internet have been effected by a TCP SYN Flood denial of service attack, prevalently termed SYN Flooding [2].

The TCP 3 way handshake is a functionality used by TCP clients and servers for synchronizing and establishing connectivity before the actual data transfer. There are three stages of TCP 3 way handshake. TCP client initiates a connection request to TCP server with the SYN bit set in the flags in the TCP header. The TCP server on receipt of the TCP SYN segment responds with a TCP segment with TCP SYN and Ack bit set in the flags. The TCP client on receipt of the above TCP segment responds with a TCP segment with the ACK bit set in the flags.

In a TCP SYN flood attack, the attacker exploits this behavior of the TCP protocol. The attacker crafts a TCP segment with the SYN bit set and sends it to the corresponding server. The server on receipt of the same would respond with a TCP segment with the SYN and Ack bit set. The corresponding state of the TCP connection in the TCP state table of the server would now progress to the SYN-RECEIVED state. The server would now be waiting for the receipt of the TCP segment with the ACK bit set, for completing the TCP 3 way handshake and progress to the ESTABLISHED state. This is also referred to as TCP Half open state or embryonic connection, which refers to as a TCP connection which is in the progress of being established. In TCP SYN flood attack, the goal of the attacker is to fill up the TCP half open states, which are allowed for the system. When the maximum numbers of half open states are filled up in memory, the connection requests from legitimate users are dropped and the server run out of resources resulting crashing, creating a Denial of Service for the application for valid users. [3].

In 2011, Subramani [4] did a test bed experiment on Distributed Denial of service attack using TCP SYN Attack, UDP Attack and ping of death attack. The network set up consisted of a router, connected to two switches with a legitimate computer, a victim, and attacker PC. They used Hyenane packet generator to test the impact of defense against the attack. Two defenses used were Rate Limiting and ACL(Access Control List). They measured RTT (Round Trip Time) delay and the results showed that without the attack the average RTT was 0.834 seconds and during the attack it went up to 8.782 seconds. With rate limiting the average RTT was

6.985 seconds and with ACL it was 1.093 seconds. They also measured the network traffic rate. During the attack it was 3216.389 kbps and without attack it was 241 Kbps. With ACL defense, it was 497kbps and with rate limiting it was 812 kbps. The results suggested that ACL is better defense than the rate limiting.

In 2012 Kaur et al [5], proposed a test bed experiment on TCP and UDP DDoS flood attacks. The test bed consisted of three computers connected to one router. One of the computers acts as a legitimate user, one as an attacker, and third computer as a victim which is a FTP server. The purpose of this study was to show the impact on the throughput during UDP and TCP attack. The results show there was a large increase in the throughput because there was larger request traffic than the legitimate users sent. In term of TCP flood attacks, before the attack the legitimate user throughput was around 75 Kbps and during the attack it was raised to double its amount reaching to 170 kbps.

There has been little work done up till now on defenses such as ACL and Rate limiting with apache server. There was also no work on the latest version of webserver, Internet Information Services 8 (IIS8). The motivation behind this paper is therefore to focuses on comparing the latest defense techniques against TCP SYN attack and establishes which defense is the best. Also this paper shows if the new IIS8 security is strong enough to stand against such an attack.

The organization of this paper is as follow. In next section the network set up is discussed. Section three covers information regarding the data generation and traffic measurement tool. Section four covers the identified defenses' mechanism which will be used in this paper. Section five will cover the analysis of the result and the last section includes conclusion, future work and acknowledgments followed by the references.

II. Network Setup

Network set up is shown in Figure 1. The test-bed was designated to simulate a real live implementation of TCP DDoS Attack. There are three types of machine in the test-bed. One computer will act as victim, second as monitoring and testing computer, and third is the two computers that initiate attacks. According to [7] in DDoS, multiple computers take part to flood a device with requests. In order to fulfill this, two attackers machine was used. Network set-up was consistent with similar research done in the past including the research in [6]. The victim machine has Microsoft Windows 2012 Server installed with web server IIS8 (Internet Information Services 8) application installed on it, which is the lasted version of Microsoft server. The machine where the attacker performs its attack has Linux Backtrack R3 installed on it that was a requirement of the software used for the attacks. Many papers with DDoS test-bed have used Linux system to attack as it consists of an exclusive tool to generate packets.

The Monitoring PC holds Windows 7 is where the monitoring tools are installed to perform network testing analysis. This machine will also act as a legitimate user.

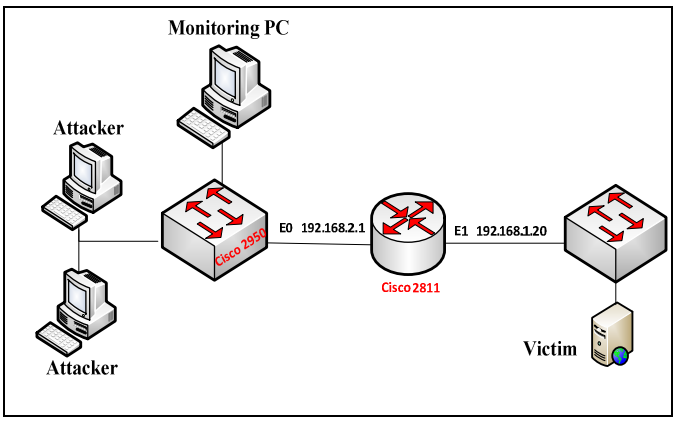

Figure 1: Test-bed For TCP SYN Flood

The computers benchmark comprised of an Intel® Core™ 5 Duo 3.40 GHz processor with 8.00 GB RAM for the efficient processing of operating system, Switch cisco 2950 and Router 2811 was chosen as the appropriate connection between the nodes. The router 2811 was used to have a spread network as well as it includes facilities to monitor the traffic in the network. The router in addition will be used for defensive purposes against the attacks. The Rip protocol was used in the router to initiate the connection. The proposed network test-bed was setup through a direct connection via standard category 5e cabling among the machines.

III. Data Generation and Traffic Measurement Tool

The last version of Hping3 [8] was chosen as an attacker traffic generator. Hping3 is considered as a real life penetration tool. Another packet generator used was Web stress tools [9]. This tools was used to send the legitimate traffic over the network and this was installed in the monitoring or user PC. For measuring the traffic, RTT was measured with an open source tool Tcping [10] and was used in the monitoring or user PC. Netflow analyzer, is another tool owned by cisco to monitor the traffic rate bandwidth in the network. Wirshark [11] was the primary tool used to capture the packet sent over the network. It was installed on the victim machine to capture incoming packets. These tools were used in many similar researches [12].

IV. Defense Mechanism

According to [13], all the efficient defenses for countering SYN flooding attacks can be approximately categorized into four: firewall-based, server-based, agent-based and router-based. The firewall based will act on behalf of the services the packet needs to be inspected before it goes to the desired server. Server based mechanism is where server monitor keeps the table of incomplete queued connections and so the server removes the need to watch for half-open connections. Examples are Sync cache [14] and SYN cookies [15]. Agent-based [16] is software developed for mitigating the impact of SYN flooding attacks. This software will continuously

monitoring the TCP three-way handshake messages before the server reply. Router-based distributed packet filtering (DPF) mechanism [17] exploits routing information to determine if a packet arriving at the router is valid with respect to its inscribed source/destination addresses.

In our experiments, we have chosen three types of categorized defense, the first one is router based defense which consist of a new technique RPF (Reverse Path Forwarding), TCP Intercept [18], ACL (Access list) and Rate Limiting Defense. The other defense is Firewall based which include TMG (Threat Management Gateway) Proxy [19]. For agent-based we have chosen new software known as Anti DDoS Guardian [20]. The following explain the defenses in more detail.

i. The TCP Intercept [18] feature on the Cisco firewall was used for the first defense. There are two modes for TCP intercept feature. The intercept mode, as the name suggests, intercepts TCP connections which are incoming to the target system. The router on receipt of the connection would respond, impersonating the server to the client. Only on successful completion of the TCP three way handshake, the server is allowed the actual connection. In our experiment, we have implement TCP intercept mode in router by using the command line (a script). This feature should eliminate malicious traffic, both spoofed IP address and that comes from TCP SYN Attack.

ii. Rate Limiting [19] is the second defense evaluated. It places a cap or sets up a threshold limit of traffic that sever would be able to withstand. The best feature of this technique is that the network administrator is allowed to decide how much traffic to be let inside the network Cisco Router. In our experiment we have Limit traffic by choosing the number of bytes required to request the webpage.

iii. The third defense was using ACL [19] known as IP addresses ingress filtering. The most commonly spoofed IP addresses are private IP addresses and other types of shared/special IP addresses. This technique will block any private IP address from entering the local network because the private IP address should not get inside the local network. In our experiment, these are the range of IP address that is been blocked from coming into the network: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 127.0.0.0/8, 224.0.0.0/3, 169.254.0.0/16. This has been implemented in router by using ACL command line. However, since we are working on a test-bed, only the legitimate IP addresses are allowed for performance. If traffic comes from outside with one of these network addresses, it must be considered fraudulent traffic.

iv. Another defense is RPF [19] which stand for Reverse Path Forwarding. This technique works much like part of an anti-spam solution. It takes the source IP address of a packet received from the Internet and looks up to see if the router has a route in its routing table to reply to that packet. If there's no route in the routing table for a response to return to the source IP, then it is likely that it is a spoofed packet, and the router drops the packet. In our experiment, we applied the defense on a router by using command line and the results show that this defense eliminated the spoofed IP Address.

v. Another defense studied was Microsoft Forefront Threat Management Gateway [19] which is proxy server. TMG has parameters that determine traffic management coming from clients and specific port listens to web request and handles authentication. TMG Proxy has the options of stopping the flood denial of service attack for TCP, UDP and ICMP Packets. These options control TCP connection which includes TCP concurrent connections per IP Address option, TCP half-open connections option, maximum TCP connect requests per minute per IP address option, HTTP requests per minute per IP address option. In our experiment we have added the proxy server between the switch and router so when the request comes it should pass the proxy server first before going to the server straight away.

vi. We have also used agent defense with software Anti DDoS Guardian [20]. This firewall software was mainly powered to prevent several of DDoS Attacks like UDP, ICMP, and TCP Attacks. The ability of this software is to control TCP connection which includes maximum number of TCP connection per second, maximum number of TCP connection for IP address, half open connection allowed, and the maximum number of concurrent client IP addresses. In our experiment, we have installed the software agent in victim and we left the TCP connection options as default due to recommendation by the vendor.

V. Results And Analysis

In our results, three major metrics were measured the first is the average RTT which is the time taken for packet to reach its destination and return back to source. In RTT we can observe the delay between the request and response time. RTT is an important metrics for establishing TCP Connection [24]. The other metric is CPU utilization of the victim. Other researches show this is important as it can crash the system [25]. But we wanted to see how much CPU utilization was affected in a modern web server which we implemented (IIS8). The last measurement was the bandwidth. As mentioned before the flood attack affects the network by consuming the bandwidth. We then compare the defenses based on these parameters.

Traffic was generated for 5 minutes (one run) and RTT, CPU utilization, and bandwidth was measured using the monitoring software explained earlier. The runs was continued for over 20runs and the results averaged and standard

deviation was measured. Runs continued until standard deviation was 0.05% of the average results.

The experiment started by using The Web stress tool to send legitimate packets from 5 users with a delay of 5 seconds between each users and then launching both attackers and defenses to see the impact. We used Wireshark to capture the incoming packet and allocate the number of packets before and after the attack for each run (5 minutes). It was found that the legitimate user send only 8 packets per second and has generated traffic 32,925 Bytes while accessing the web page. The attacker flooded the network with almost 25000 packets per second and has generated traffic 128581552 Bytes.

Average RTT Results

Table 1 shows that for legitimate users the average RTT was 1.92ms before the attack, while, during the TCP SYN Attack the average RTT was around 5252.52ms. This happened due to thousands of packet jamming the network which resulted in longer delays than usual.

Scenario	Average RTT(ms)
Without an attack	1.92 ms
During the attack	5252.52 ms
With TCP Intercept	3.21 ms
With Rate Limiting	3749.68 ms
With Access List	3098.65 ms
With Reverse Path Forwarding	2728.26 ms
Anti DDOS Guardian	2553.71 ms
Forefront TMG Proxy 2010	2803.34 ms

Table 1: Average RTT before attack, during attack, and various defenses

It was noted that TCP Intercept was the most effective defense among the other defenses implemented, as it resulted in the average RTT to be 3.21 ms. This is because TCP Intercept eliminated malicious SYN attack traffic spoofed from reaching the server. Rate limiting resulted in the highest RTT. This happened, as mentioned earlier, rate limiting does not block the malicious traffic, it only limits the traffic to the threshold. ACL was the second worst defense with RTT of 3098.65 ms. Both anti DDoS and TMG Proxy have RTT 2553.71 ms and 2803.34 ms respectively. The RTT of both anti DDoS and TMG Proxy gave high RTT, because they only drop the malicious when it comes but did not actually stopped the flooding. RPF defense almost halved RTT during attack (from 5252ms to 2553ms). It only stopped the spoofed IP address traffic not the attacker with a valid IP that can come from Zombies.

CPU Utilization in the Target system

TCP SYN Attack affect the CPU untilisation of the target system because the web server needs to proccess the requests and queue them as there are many requests per second. As mentioned earlier, other research shows TCP SYN attack on some webservers can result in crashing of the system due to high CPU utlisation.

Scenario	Utilization
During TCP SYN Attack	10 %
Without an attack	1 %
With TCP Intercept	1 %
With Rate Limiting	9 %
With Access List	9 %
With Reverse Path Forwarding	7 %
Anti DDOS Guardian	50 %
Forefront TMG Proxy 2010	1 %

Table 2: CPU Utilization before attack, during attack, and various defenses

As we can see from Table 2, the CPU Utilisation percentage was 1 % before attack but it jumped up to 10 % during TCP SYN Attack. It was very surprising to see that IIS8 was able to hold up against the attack. In terms of defence, we discovered that TCP Intercept had completely eliminated the maclious traffic from passing the router and going to the webserver. This is quite similar to TMG Proxy in which it has protected the server from getting damaged from TCP SYN Attack. However, we learned that during the attack the proxy server's CPU itself went up to 60%. Both rate limiting and ACL have CPU utilisation of 9% because rate limiting allows passing the packets and ACL eliminates the maclious packets but still some packets do manage to pass through. RPF resulsts in 7% of the target system CPU. The highest CPU utilisation percentage was when Anti DDOS Guardian was used which reslusted in 50% because it was installed in the viticm machien.

Average Network Bandwidth

The more traffic there is the more the bandwidth will be consumed.

Scenario	Traffic Rate (Kbps)
During TCP SYN Attack	776.51
Without an attack	1.342
With TCP Intercept	1.462
With Rate Limiting	424.07
With Access List	421.65
With Reverse Path Forwarding	388.26
Anti DDOS Guardian	630.30
Forefront TMG Proxy 2010	610.16

Table 3: Average Traffic Rate before attack, during attack, and various defenses**.**

It can be noted from Table 3 that the traffic rate bandwidth without the attack is 1.342Kbps but during the attack it has significantly increased to 776.51Kbps which results in the legitimate user struggling to access the webserver. It can be observed that there is not much significant difference between TCP Intercept traffic rate average bandwidth and the

legitimate traffic bandwidth as the defenses have dropped the connection before it enters the network which results in 1.462 Kbps traffic rate. The proxy server is another defense which eliminates malicious traffic resulting in network traffic rate of 610.16Kbps. This is due to proxy server eliminating the packets from reaching the server only. However it doesn't actually drop the traffic from getting into the network. This is also the case for Anti DDOS Guardian which results in similar bandwidth as the proxy server. It just eliminates traffic within the victim machine but does let some packets pass through. ACL and Reverse Path Forwarding dropped the traffic to 421.65Kbps and 388.26Kbps respectively. Rate Limiting has the traffic rate bandwidth of 424.07Kbps as it allowed the traffic but with some threshold limit.

VI. CONCLUSION

During our experiments we established that the most destructive side of the SYN attack was to consume the bandwidth of the network which made legitimate users take longer time to access the destination system. Looking into the three mercies we have measured we could define the best and the worst defense. TCP Intercept is the best option to protect from network consumption and appliances as it acts on behalf of the server. However the average delay still increased from 1.92ms (without attack) to 3.21 ms (with defesene). TCP intercept reduced the Victim CPU Utilization to 1% and traffic bandwidth rate only increased a bit from 1.342 (without attack) to 1.462 kbps (with defense). The worst defense depends on the metrics studied. In terms of RTT, Rate Limiting cannot be an ideal solution as it still permits controlled traffic with high RTT of 3749.68 ms. For CPU utilisation, Rate limiting and ACL only made the Utilization of Victim CPU to 9%. However Anti DDoS Guardian has increased almost 50% the CPU.. Surprisingly in bandwith evaluation, Anti DDoS Guardian was the worst. It increased the traffic rate from 1.342 Kbps (without attack) to 630.30 Kbps (with defesene). Because it did not stop the attack but drop the traffic coming into the victim's computer. So we conclude that in router based filtering, TCP intercept is the best defense and the worst is the Rate Limiting. Among all the defenses category Anti DDoS Guardian is the worst.

VII. FUTURE WORKS

Since IPv4 is disappearing and is getting substituted by IPv6, the future work must emphasis on stopping DDoS in IPv6. Although additional headers and options for improved security in IPv6, it is still susceptible to numerous Denial of Service attacks. Thus further research effort should be emphasized on IPv6 security and suitable mitigation techniques should be introduced for prevailing vulnerabilities.

ACKNOWLEDGMENT

The authors would like to thank UNITEC Institute of Technology for funding the research team and providing the inventory needed.

REFERENCES

[1] Eddy, W. M. (2006). Defenses Against TCP SYN Flooding Attacks. The Internet Protocol Journal, 9.

[2] B. B. Gupta, R. C. J., Manoj Misra. (2010). Distributed Denial of Service Prevention Techniques. International Journal of Computer and Electrical Engineering, 2.

[3] Ohsita, Y., Ata, S., & Murata, M. (2012.). Detecting distributed denial-of-service attacks by analyzing TCP SYN packets statistically. Global Telecommunications Conference, 2004. GLOBECOM. IEEE, 4, 2043 - 2049.

[4] Subramani rao Sridhar rao, D. M. R. (2011). Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis. School of Computer Science and Electronic Engineering, University of Essex.

[5] Kaur , D., Sachdeva , M., & Kumar , K. (2012). Study of DDoS attacks using DETER Testbed. International Journal of Computing and Business Research (IJCBR) ISSN (Online) : 2229-6166, 3(2).

[6] Viecco, C., & Camp, J. (2008). A Life or Death InfoSec Subversion. Security & Privacy,IEEE, 6(5), 74 - 76.

[7] Garber, L. (2000). Denial-of-Service Attacks Rip the Internet Technology News. TECHNOLOGY NEWS, 12-17

[8] Oriyano, S. -P., & Gregg, M. (2011). Hacker techniques, tools, and incident handling. Sudbury, Mass: Jones & Bartlett Learning.

[9] Bai, Y.-W. W. (2004). A two-pass web document allocation method for load balancing in the multiple grouping of a Web cluster system IEEE Xplore 1, 177 – 181

[10] Mase K., N. U., Tsuno, A, Toyama, Y., Karasawa, N. . (2001). A Web server selection algorithm using QoS measurement Communications, 2001. ICC 2001. IEEE International Conference, 8, 2332 - 2336 .

[11] Rastogi, D., Ganu, S., Zhang, Y., Trappe, W., & Graff, C. (2007). A Comparative Study of AODV and OLSR on the ORBIT Testbed. Military Communications Conference, IEEE, 1 - 7. Retrieved from

[12] Yujie , P., & Hongbo , W. (2009). A passive method to estimate TCP round trip time from non sender-side. Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, 43-47

[13] Peng , T., Leckie , C., & Ramamohanarao, K. (2004). Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring. In Proceedings of the Third International IFIP-TC6 Networking Conference

[14] Lemon, J. (2002). Resisting SYN Flooding DoS Attacks with a SYN Cache. Proceeding BSDC'02 Proceedings of the BSD Conference 2002 on BSD Conference, 10

[15] D. J. Bernstein and Eric Schenk, "Linux Kernel SYN Cookies Firewall Project", http://www.bronzesoft.org/projects/scfw

[16] C. L. Schuba, I. V . Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram andD. Zamboni, " Analysis of a Denial of Service Attack on TCP", Proceed-ings of IEEE Symposium on Security and Privacy, May 1997

[17] Gupta, B., Joshi, R. C., & Misra, M. (2010). Distributed Denial of Service Prevention Techniques. International Journal of Computer and Electrical Engineering, 2, 9.

[18] Cisco IOS Security Command Reference, Release 12.2 - TCP Intercept Commands [Cisco IOS Software Releases 12.2 Mainline] - Cisco Systems.(2013).Retrieved from http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/srfenl.html

[19] Microsoft Forefront. Retrieved 20/04/2013, 2013, from http://technet.microsoft.com/en-us/library/cc995196.aspx

[20] Anti DDoS | DDos Protection for Windows Servers free downloads. (2013). Retrieved from http://www.beethink.com/antiddos.htm