Journal of Information Security, **2011, 2, 50-58**
doi:10.4236/jis.2011.21005 Published Online January 2011 (http://www.SciRP.org/journal/jis)

Experimental Evaluation of Juniper Network's Netscreen-5GT Security Device against Layer4 Flood Attacks

Sanjeev Kumar, Raja Sekhar Reddy Gade
Network Security Research Lab, Department of Electrical and Computer Engineering,
The University of Texas–Pan American, Edinburg, USA
E-mail: *sjk@utpa.edu*

Received September 29, 2010; *revised December* 11, 2010; *accepted January* 15, 2011

Abstract

Cyber attacks are continuing to hamper working of Internet services despite increased use of network security systems such as firewalls and Intrusion protection systems (IPS). Recent Distributed Denial of Service (DDoS) attacks on Dec 8th, 2010 by Wikileak supporters on Visa and Master Card websites made headlines on prime news channels all over the world. Another famous DDoS attacks on Independence Day weekend, on July 4th, 2009 were launched to debilitate the US and South Korean governments' websites. These attacks raised questions about the capabilities of the security systems that were used in the network to counteract such attacks. Firewall and IPS security systems are commonly used today as a front line defense mechanism to defend against DDoS attacks. In many deployments, performances of these security devices are seldom evaluated for their effectiveness. Different security devices perform differently in stopping DDoS attacks. In this paper, we intend to drive the point that it is important to evaluate the capability of Firewall or IPS security devices before they are deployed to protect a network or a server against DDoS attacks. In this paper, we evaluate the effectiveness of a security device called Netscreen 5GT (or NS-5GT) from Juniper Networks under Layer-4 flood attacks at different attack loads. This security device NS-5GT comes with a feature called TCP-SYN proxy protection to protect against TCP-SYN based DDoS attacks, and UDP protection feature to protect against UDP flood attacks. By looking at these security features from the equipments data sheet, one might assume the device to protect the network against such DDoS attacks. In this paper, we conducted real experiments to measure the performance of this security device NS-5GT under the TCP SYN and UDP flood attacks and test the performance of these protection features. It was found that the Juniper's NS-5GT mitigated the effect of DDoS traffic to some extent especially when the attack of lower intensity. However, the device was unable to provide any protection against Layer4 flood attacks when the load exceeded 40Mbps. In order to guarantee a measured level of security, it is important for the network managers to measure the actual capabilities of a security device, using real attack traffic, before they are deployed to protect a critical information infrastructure.

Keywords: Distributed Denial of Service (DDoS), TCP-SYN Flood Attack, TCP-SYN Proxy Protection, Firewall Security, UDP Flood Attack

1. Introduction

Internet is the foremost leading media for multimedia information exchange today. However, the ease of Internet communication comes with the threat of security attacks, which are known to disrupt such communications over Internet. As recently as Dec. 8th, 2010, the servers of Visa, MasterCard, PayPal and several others were brought down by the supporters of WikiLeaks using DDoS attacks [1]. On August 6th 2009, servers like Twitter, Facebook, Live journal, Google's Blogger and Youtube were under DDoS attacks, where Twitter was down for several hours [2]. According to CSI Computer and Security Survey 2008, Firewall type of security technology was used by 94% of the organizations [3]. Many manufacturers are designing firewalls and advanced security devices to provide increased protection for their customers from different types of attacks. Despite widespread use of firewalls to protect corporate and government websites, the damage caused by the denial of service attacks do not seem to have gone away completely. The DDoS attacks, launched during Wikileaks related events starting Dec. 8th, 2010, and the Independence Day DDoS attacks on July 4th, 2009 launched against US and South Korean government websites [4], are now prompting many network managers to question the performance of their firewalls, IPS or other Internet security devices being used in defending against such DDoS attacks [5-13]. In this paper, we evaluate performance of Juniper Network's NetScreen NS-5GT Internet security device [14,15] to measure its effectiveness in defending against two popular layer-4 DDoS attacks, namely the TCP-SYN and UDP flood attacks. The rest of the paper is organized as follows: Section 2 has a discussion on the TCP and UDP flood attacks that are evaluated in this paper, and the protection mechanisms offered by the Juniper Network's NS-5GT security device to protect against these two DDoS attacks. Section 3 provides detail of experimental setup, different scenarios of protection used in the experiments, and discussion on respective results. Section 4 concludes the paper.

2. Juniper's Netscreen NS-5gt Internet Security Device

The Juniper's NetScreen 5GT (NS-5GT) is an Internet Security device that combines functionalities of firewall, Intrusion Prevention System (IPS), VPN and traffic shaping functions [14,15]. NS-5GT device is an enterprise class security solution designed to defend against various security attacks including layer-4 DDoS attacks such as TCP-SYN flood or UDP-flood attacks.

2.1. TCP-SYN Flood Attack

In this type of DDoS attack, the attacker sends a flood of TCP-SYN packets with spoofed addresses. The server responds with corresponding SYN-ACK packets which are never answered with the final ACK packets.

This results in establishment of numerous half open connections at the victim computer (**Figure 1**), which causes excessive consumption of computing resources of the victim computer. This type of DDoS attack is called TCP-SYN flood attack. During this attack, legitimate client connections are dropped as a result of lack of computing resource at the victim computer.

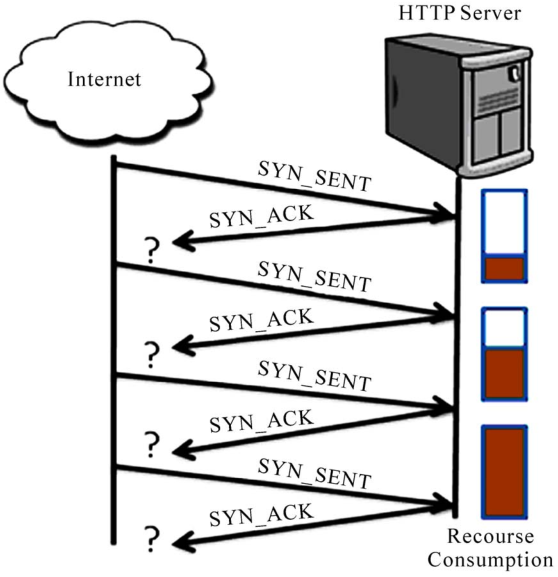


Figure 1. TCP SYN flood attack.

2.2. Protection Provided by NetScreen NS-5GT against TCP-SYN Based DDoS Attacks

The security device NS-5GT from Juniper Networks provides protection against TCP-SYN based DDoS attacks by using a mechanism called SYN Proxy protection method [14,15]. According to this mechanism, the NS-5GT Internet security device is placed between the server (that needs to be protected) and the Internet. In this position, the NS-5GT does the proxy on behalf of the server and participates in the initial TCP 3-Way Handshake process (**Figure 2**) to authenticate genuine client connections to the server.

According to this protection mechanism, first a SYN attack threshold is set in the NS-5GT, which is an upper limit on the number of SYN segments permitted through the device per second. If this threshold is exceeded, then the NS-5GT starts to proxy on behalf of the server and directly participates in 3-way handshake with the clients, to establish a legitimate connection. The NS-5GT replies with SYN_ACK to the initial SYN segments arriving from the clients, and hence opening up a number of half open connections. In the case of genuine client connections, the final ACK segment is sent from the client, and upon receiving it the security device NS-5GT forwards it to the server for establishment of a secure TCP connection. If the final ACK segment doesn't arrive then the half open connection at the intermediate NS-5GT device is terminated or timed out.

2.3. UDP Flood Attack

UDP is another common Layer-4 traffic on internet.

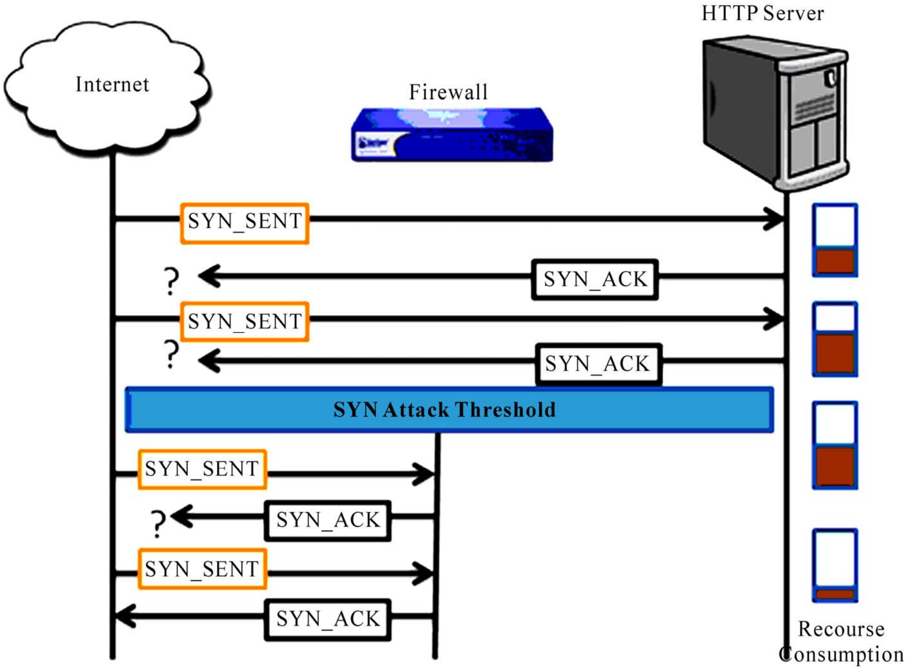


Figure 2. SYN Proxy protection [15].

However unlike TCP traffic, the Web-servers do not receive a lot of UDP traffic. During UDP flood attacks, a flood of UDP packets are sent to the victim computers either on specified ports or on random ports. The victim computer or server processing those UDP packets replies with valid information, if there is an application available on the specified port, otherwise the victim computer sends "ICMP Destination Unreachable" message to the spoofed sender. UDP flood attacks can also consume computing resources on the victim system besides the bandwidth. The Juniper's NetScreen NS-5GT security device also has a protection feature that claims to protect against UDP flood attacks. In this paper, we measure the capability of the NS-5GT to defend against UDP flood attacks.

2.4. Protection Provided by NetScreen NS-5GT against UDP-Flood Based DDoS Attacks

The NetScreen 5GT provides protection against UDP flood attacks by monitoring the rate of incoming UDP datagrams to the NS-5GT. The security device NS-5GT passes the UDP datagrams only if a policy permits them. For example, as shown in **Figure 3**, the UDP packet can be targeted to a DNS server.

In the case of attack, the attacker sends a flood of UDP datagrams to a DNS server, which rides IP packets with spoofed source addresses. The security device protects against this type of UDP flood attack by imposing a limit on the maximum rate i.e. the maximum number of UDP datagrams that can be allowed to pass through the security device per second. After the threshold is crossed, the security device NS-5GT starts dropping all UDP datagrams from all source addresses and destined to the same subnet for the remaining second and also for the next successive second. During this time period when the threshold is enabled, the UDP packets from the legitimate clients are also dropped. Thus the dropping of all UDP datagrams stays in effect, as long the threshold limit stays violated by the flood of incoming UDP packets.

3. Experimental Setup and Measurements

For experiments, an evaluation network was set up in a controlled lab environment as shown in **Figure 4**, where we launched a TCP-SYN attack and UDP flood attack to measure the performance of Juniper's Netscreen 5GT Security Device. The number of client connections established per second to the server was used as the performance parameter in these experiments. In these experiments, we measured the number of client connections per second against different loads of attack traffic. To compare the effectiveness of the security device, the performance was evaluated with and without respective protections being enabled on the NS-5GT security device to stop the flood attacks from reaching the server. For this experiment, along with the Juniper Networks NS-5GT security device, the Windows Server 2003 with Intel® Xeon^{TM} 3GHz Processor and 4GB RAM were used.

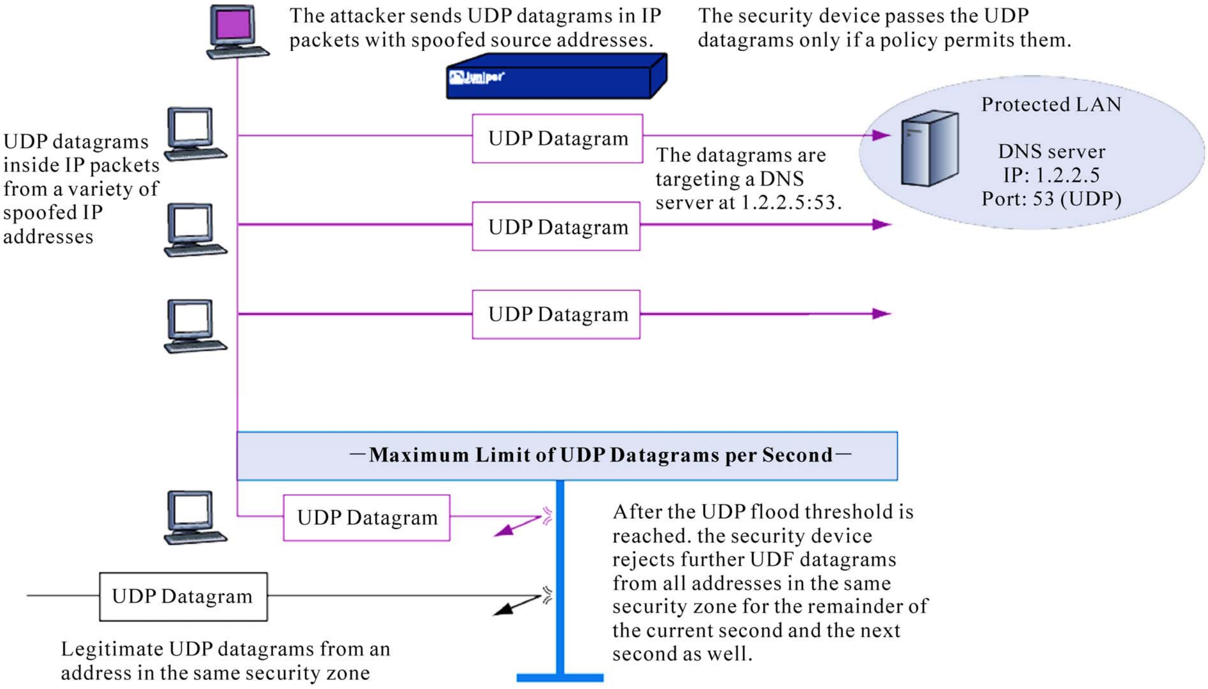

The attacker sends UDP datagrams in IP packets with spoofed source addresses.
The security device passes the UDP datagrams only if a policy permits them.
Juniper
Protected LAN
DNS server
IP: 1.2.2.5
Port: 53 (UDP)
UDP datagrams inside IP packets from a variety of spoofed IP addresses
UDP Datagram
The datagrams are targeting a DNS server at 1.2.2.5:53.
UDP Datagram
UDP Datagram
—Maximum Limit of UDP Datagrams per Second—
UDP Datagram
UDP Datagram
After the UDP flood threshold is reached. the security device rejects further UDF datagrams from all addresses in the same security zone for the remainder of the current second and the next second as well.
Legitimate UDP datagrams from an address in the same security zone

Figure 3. UDP flood protection method used by NS-5GT [15].

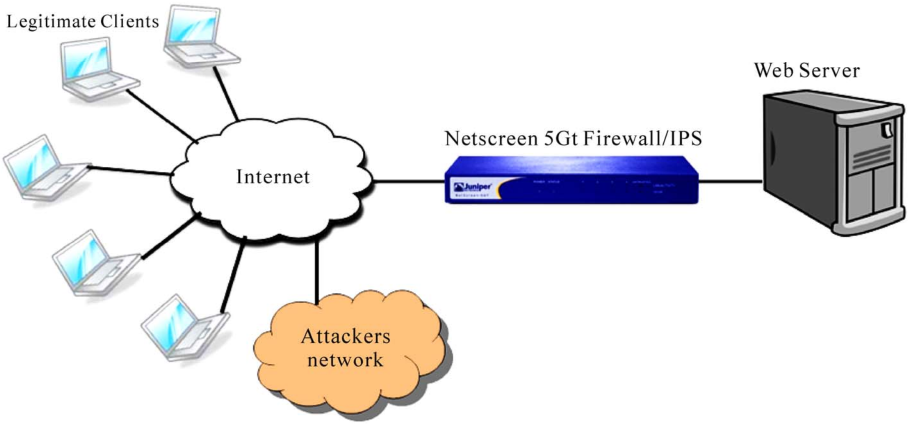


Figure 4. Experimental setup to evaluate the effectiveness of Juniper's NT-5GT security device.

The set up in **Figure 4** shows the legitimate HTTP clients that connect to the server through the security device NS-5GT. Furthermore, the attacker's network is used to simulate the Distributed Denial of Attack (DDoS) attack with the attack traffic being sent with spoofed addresses. Since the Juniper's NS-5GT security device system supported an interface of 100Mbps for internet traffic, the security device was subjected to a range of layer-4 attack traffic load up to 100Mbps.

Prior to starting the experiments, we first measure the baseline performance of the security device NS-5GT in supporting the maximum number of stable client connections per second in the absence of any attack traffic. In the absence of any attack traffic, the maximum number of stable client connection rate established with the server through the NS-5GT security device was measured to be 600 connections per second (baseline performance of the NS-5GT security device).

3.1. TCP SYN Attack on Server without Protection Enabled on Juniper's NS-5GT Security Device

In this case, the security device NS-5GT was setup with no proxy protection enabled against TCP-SYN attacks. A stable connection rate of 600 legitimate client connections per second was established with the server during the experiment. The TCP-SYN attack, with the attack load varying from 10 Mbps to 100Mbps was launched on the server with no SYN proxy protection enabled at the NS-5GT security device. We measured the number of connections per second formed with the end server through the NS-5GT under different loads of TCP-SYN flood attack (**Figure 5**).

Based on the experimental measurements, it was found that the number of legitimate client connection rate was brought down to around 176 connections/sec from the baseline rate of 600 connections/sec under the TCP-SYN attack load of only 15 Mbps. Furthermore, the number of legitimate client connections was brought down to zero when the attack load was increased to 20 Mbps. The number of client connection rate established with the server through the NS-5GT security device (used as a gateway) at different attack loads is shown in **Figure 5**.

3.2. TCP-SYN Attack on Server with SYN-Proxy Protection Enabled on Juniper's NS-5GT Security Device

In this case, the SYN Proxy protection was enabled on the NS-5GT, with default threshold value on the number of TCP SYN permitted through the security device. Despite enabling of the SYN proxy protection, we found that the client connections rate dropped to zero at 45 Mbps of SYN flood attack traffic load as shown in **Figure 6**.

Based on the measurements done for the client connection rate that can be supported with and without TCP proxy protection enabled at the Juniper's NS-5GT security device, such comparison is shown in **Figure 7**. The green bar on the left in **Figure 7** shows the number of successful client connections formed per second without SYN proxy protection enabled at the NS-5GT, whereas the blue bar on the right in **Figure 7** shows the number of successful client connections formed per second with SYN proxy protection enabled at the Juniper's NS-5GT security device.

On one hand, it can be seen that without SYN-proxy protection being enabled at the NS-5GT security device, the legitimate client connection rate fell sharply to zero around 20 Mbps of TCP-SYN attack traffic. On the other hand, it can be seen that when the SYN-proxy protection

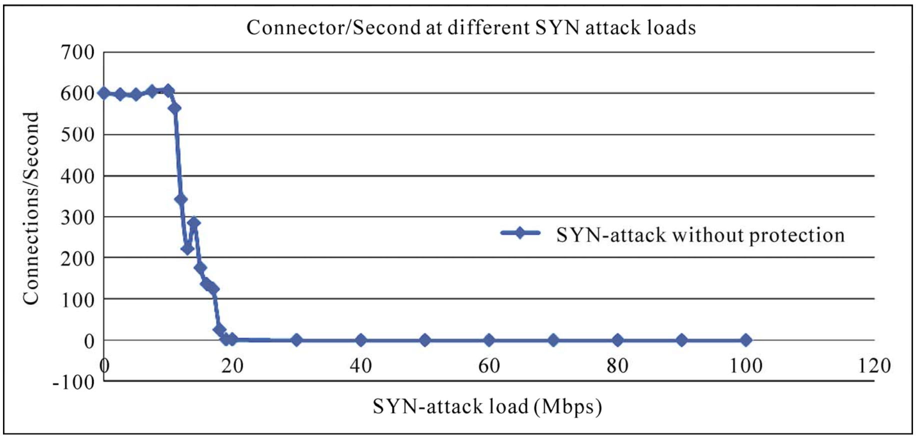


Figure 5. Client connection rate under different TCP-SYN attack loads with no protection enabled on NS-5GT.

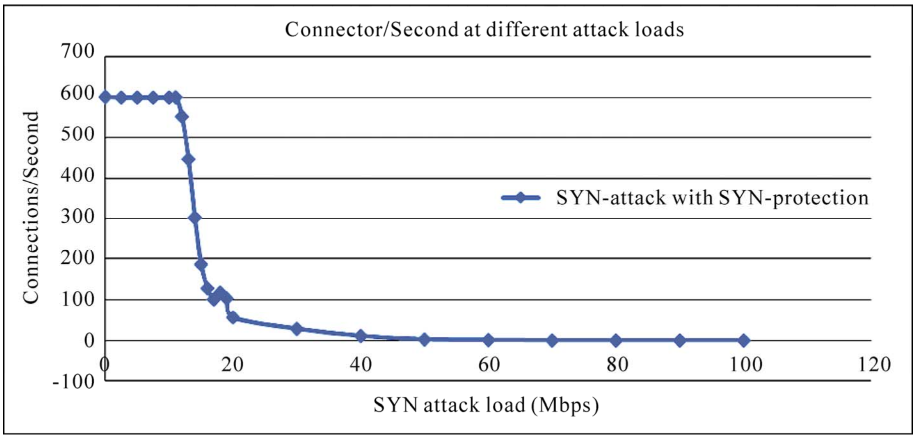
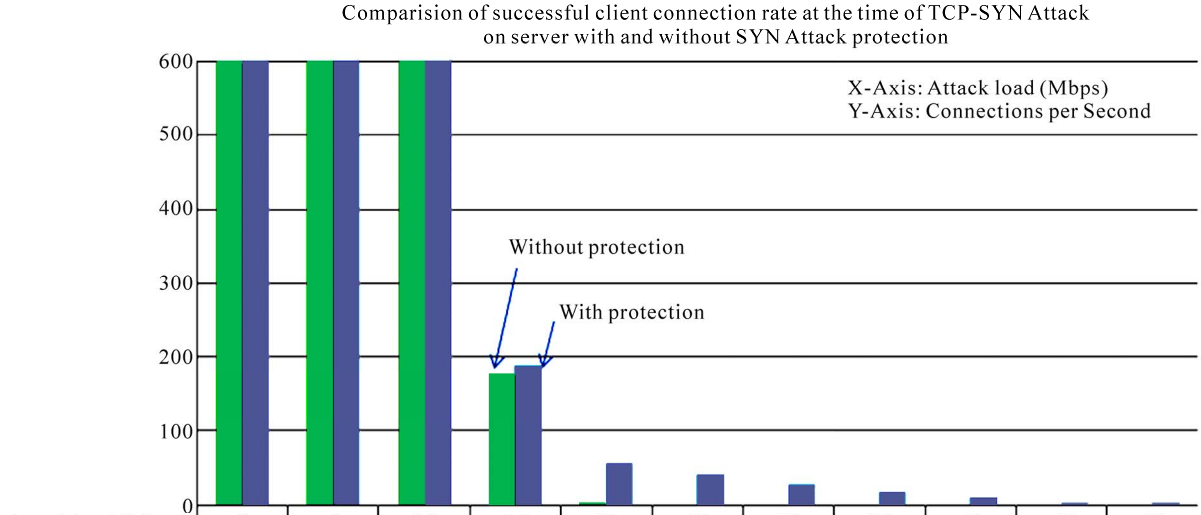


Figure 6. Client connection rate under different TCP-SYN attack loads with SYN-proxy protection enabled on NS-5GT.



Attack load (Mbps)	0	5	10	15	20	25	30	35	40	45	50
🟩Without protection	600	600	600	176	2	0	0	0	0	0	0
🟦With protection	600	600	600	187	56	41	28	17	11	2	1

Figure 7. Connections per second compared with and without SYN Proxy protection enabled on the Juniper's NS-5GT security device.

was enabled at the Juniper's NS-5GT security device, it took 45 Mpbs of TCP-SYN attack traffic to completely deny legitimate client connections through the Juniper's Netscreen 5GT security device.

Comparative study and results (**Figure 7**) show that the security effectiveness provided by the Juniper's NS-5GT security device is very marginal in improving the client connection rate, and almost ineffective in protecting against TCP-SYN attacks of higher intensity exceeding 45 Mbps. It is obvious that the security device NS-5GT from Juniper Networks is not capable enough to protect against high intensity TCP-SYN attacks despite offering protection features against such attacks.

3.3. UDP Flood Attack on Server without UDP-Flood Protection Enabled on Juniper's NS-5GT Security Device

In this case, we study the effectiveness of the Juniper's security device NS-5GT in protecting against UDP flood attack. For comparison of its protection mechanism, we consider two scenarios to measure the effect of security provided by the NS-5GT on the connection rate–first scenario, when the UDP flood attack is launched without enabling the UDP flood protection at NS-5GT. Second scenario, when the UDP flood attack is launched after enabling the UDP flood protection at NS-5GT. In this section, we cover the first scenario when the security device NS-5GT was setup with no UDP-flood protection, and the server maintained an initial (baseline) client connection rate of 600 connections per second during the experiments. The UDP flood attack traffic varying from 10 Mbps to 100 Mbps in steps of 10 Mbps was sent towards the server through the security device NS-5GT. The effect of attack traffic loads on the client connection rate was measured and plotted in **Figure 8**.

When the server is flooded with the spoofed UDP traffic, the UDP packet received by the server processes the packets and checks for the application on the requested port number. If there was no application found on that requested port then the server sends the destination unreachable packet as reply for the received packets.

Results in **Figure 8** show that the number of client connections dropped to half of its maximum baseline capacity under UDP flood attack load of 35 Mbps. Furthermore, without UDP flood protection on the NS-5GT security device, no client connection could be established under UDP attack load of 40 Mbps or higher.

3.4. UDP Flood Attack on Server with UDP Flood Protection Enabled on Juniper's Security Device NS-5GT

In this case, the UDP flood attack protection (**Figure 3**) was enabled on the Juniper's NS-5GT security device to evaluate its effectiveness in mitigating the attack, and in improving the number of client connections under UDP flood attack conditions. Initially, in the absence of attack conditions, the baseline client connection rate of 600 connections per second was maintained during the experiment. The UDP flood attack load varying from 10 Mbps to 100 Mbps in steps of 10 Mbps was sent towards the server, through the Juniper's security device NS-5GT gateway, in order to measure its effectiveness in preventing the attack. The number of connections per second was measured against different loads of attack.

When the UDP flood protection was enabled on the Juniper Networks security device NS-5GT, it was found that under an UDP attack traffic load of 30 Mbps, the connection rate dropped from baseline connection rate of 600 connections/sec to around 373 connections/sec, *i.e.* a decrease of around 38% in the baseline performance.

Whereas, without such UDP flood protection being enabled on the security device NS-5GT (**Figure 8**), only 97 connections/sec could be supported under the UDP attack load of 30 Mbps *i.e.* around 84% decrease in the baseline performance. The relative improvement in the connection rate provided by the UDP protection mechanism of the security device can be calculated as 46% for the attack load of 30 Mbps. It can be seen that at lower attack loads, there was some improvement in the connection rate provided by the security device NS-5GT, however when the UDP attack load was increased to 45Mbps or higher, no client connections could be established *i.e.* 0% improvement in the connection rate despite claims of providing protection against UDP attacks by the NS-5GT security device.

The results show that the NS-5GT provides some protection against the UDP flood attack of lower intensity (below 40 Mbps), however it is not effective in preventing against UDP flood attacks of higher intensity (*i.e.* exceeding 40 Mbps).

Based on the measurements done for the number of client connection rate that can be supported with and without UDP flood protection enabled at the Juniper's NS-5GT security device, we show such comparison in **Figure 10**. The green bars on the left in **Figure 10** show the number of successful client connections formed per second when no UDP flood protection was enabled at the NS-5GT. Whereas the blue bars on the right in **Figure 10** show the number of successful client connections formed per second with UDP flood protection enabled at the Juniper's NS-5GT security device.

From **Figure 10**, it can be observed that without UDP flood-protection enabled at the NS-5GT security device, the client connection rate goes to almost zero at 35 Mbps

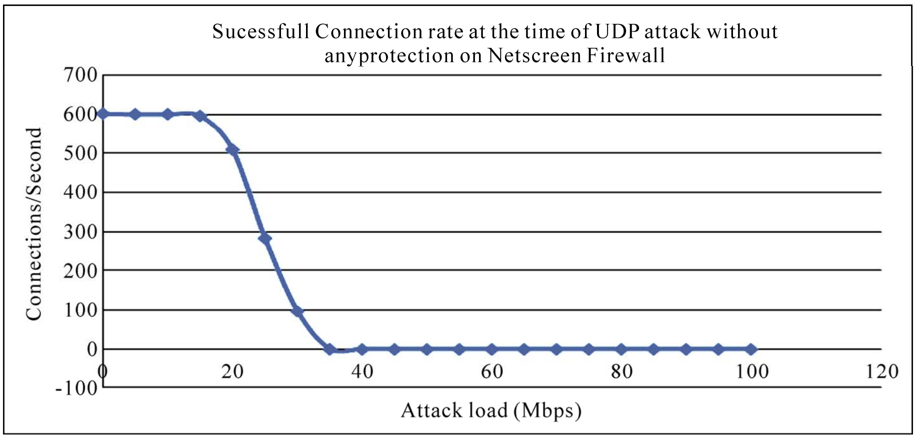


Figure 8. Client connections established under different UDP flood attack loads with no protection enabled on NS-5GT.

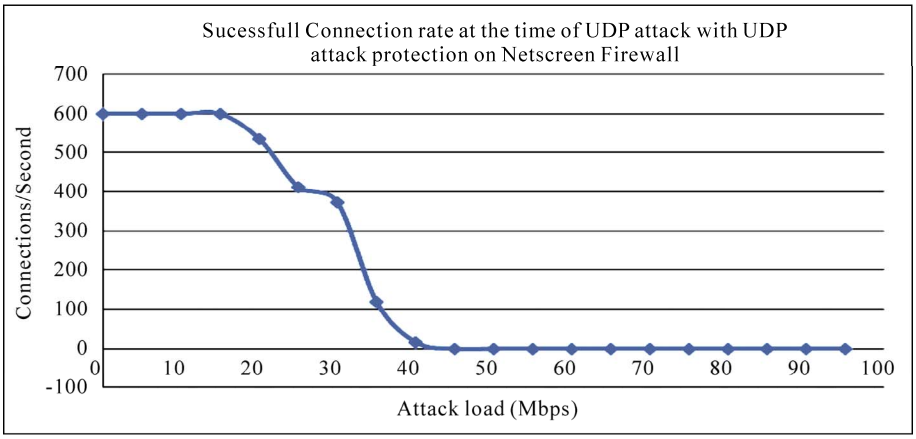
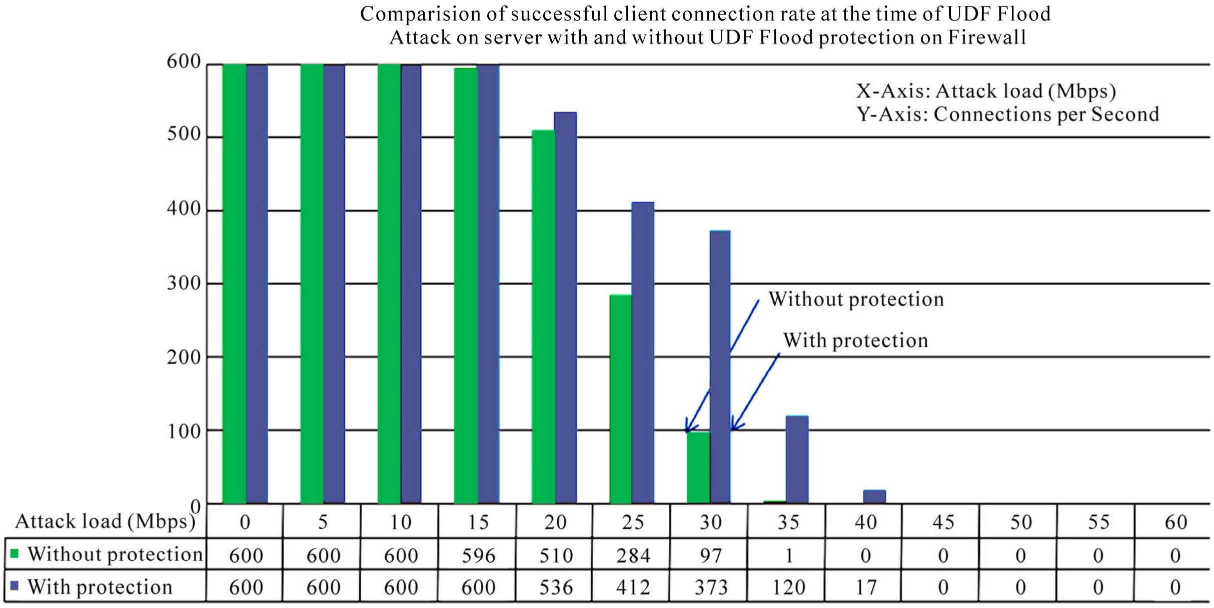


Figure 9. Client connections established under different UDP flood attack loads with UDP-protection enabled on NS-5GT.



Attack load (Mbps)	0	5	10	15	20	25	30	35	40	45	50	55	60
🟩 Without protection	600	600	600	596	510	284	97	1	0	0	0	0	0
🟦 With protection	600	600	600	600	536	412	373	120	17	0	0	0	0

Figure 10. Comparison of Connection rate with and without UDP-flood protection enabled on the NS-5GT security device.

of UDP-flood attack traffic. Whereas when the UDP-flood attack protection is enabled on the NS-5GT, the connection rate goes to zero at a little higher traffic load of 45 Mbps. The connection drop rate is found to be somewhat slower when the protection is enabled at the NS-5GT security device for lower attack loads (**Figure 10**). Overall the protection provided by the security device NS-5GT is marginal against prevention of the UDP flood attacks considered in this paper.

4. Conclusion

In this paper, we evaluated the performance of a Juniper Network security device NS-5GT to measure its effecttiveness in providing protection against Layer-4 TCP-SYN and UDP based DDoS attacks. It was found that the protection provided by NS-5GT was capable in defending to some extent against lower loads of TCP-SYN and UDP based DDoS attacks, however at higher attack loads exceeding 40 Mbps, the NS-5GT security device was not capable of establishing client connections in the face of such flood attacks. Despite the security protection offered by the security device NS-5GT, the evaluation results showed the Juniper's security device NS-5GT to be of limited capability in preventing layer4 DDoS attacks. The Juniper Network security device NS-5GT, claimed to provide protection against TCP SYN attacks and UDP flood attacks, however the protection was measured to be not effective in defending against higher intensity of such attacks exceeding 40 Mbps. Before deploying a network security device to protect a critical information infrastructure, it is important for the network administrators to seek actual performance evaluation results from the manufacturers to determine the actual capabilities of the Internet security devices in preventing against DDoS attacks.

5. Acknowledgements

This research work is based upon work supported in part by US National Science Foundation under Grant No. 0421585. Authors would like to thank Hari Vallelacheruvu and Sirisha Surisetty of the networking research lab for their helpful discussion and assistance with the experiments.

6. References

[1] "WikiLeaks Supporters Tear down VISA in DDoS Attack," December 9, 2010. http://www.digitaltrends.com/computing/wikileaks-supporters-tear-down-visa-in-ddos-attack/.

[2] Cnet news, "Twitter Crippled by Denial-of-Service Attack", 15 October 2010. http://news.cnet.com/8301-13577_3-10304633-36. html

[3] R. Richardson, "2008 CSI Computer Crime & Security Survey," CSI, 2008.

[4] "US Suspects N Korea Launched Internet Attack on July 4," 15 October 2010. http://ibnlive.in.com/news/us-suspects-n-korea-laun-ched-internettack-on-%20%20%20%20%20july-4/96715 -2.html

[5] "Computer Emergency Response Team (CERT)® Advisory CA-2001-20," 15 October 2010. http://www.cert.org/tech_tips/home_ networks.html

[6] "Computer Emergency Response Team (CERT)®,"

Trends in Denial of Service Attacks Technology. 15 October 2010. http:// www.cert.org/archive/pdf/DoS_trends.pdf

[7] C. Douligeris and A. Mitrokotsa, "DDOS Attacks and Defense Mechanisms: A Classification," *Proceedings of the* 3*rd IEEE International Symposium on Signal Processing and Information Technology*, 14-17 December 2003, pp. 190-193. doi:10.1109/ISSPIT.2003.1341092

[8] J. Mirkovic and P. Reiher. "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communications Review*, Vol. 349, No. 2, April 2004, pp. 39-54. doi:10.1145/997150.997156

[9] S. Kumar, "Smurf Based Denial of Service Attack Amplification in Internet," *IEEE Computer Society,* ICIMP, 2007.

[10] M. R. Lyu and L. K. Y. Lau, "Firewall Security: Policies, Testing and Performance Evaluation," *The* 24*th Annual International Computer Software and Applications Conference*, Taipe, 25-27 October 2000, pp. 116-121.

[11] R. K. C. Chang "Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial," *IEEE Communications*, Vol. 40, No. 10, April 2002, pp. 42-51. doi:10.1109/MCOM.2002.1039856

[12] S. Kumar, M. Azad, O. Gomez and R. Valdez, "Can Microsoft's Service Pack-2 (SP2) Security Software Prevents Smurf Attacks?" *Advanced International Conference on Telecommunications*, Guadeloupe, September 2006, pp. 89-93.

[13] S. Kumar and E. Petana, "Mitigation of TCP-SYN Attacks with Microsoft's Windows XP Service Pack2 (SP2) Software," *Seventh International Conference on Networking*, Cancun, 13-18 April 2008, pp. 238-242. doi: 10.1109/ICN.2008.77

[14] "Juniper Networks NetScreen NS 5GT Security Policy," 15 October 2010. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp629.pdf

[15] Juniper Networks, Inc., "Attack Detection and Defense Mechanisms," 2008. http://www.juniper.net/techpubs/software/screenos/screenos5x/ce_v4_5_0.pdf