Journal of Information Security, **2012, 3, 122-137**
http://dx.doi.org/10.4236/jis.2012.32015 Published Online April 2012 (http://www.SciRP.org/journal/jis)

Experimental Evaluation of Cisco ASA-5510 Intrusion Prevention System against Denial of Service Attacks

Raja Sekhar Reddy Gade, Sanjeev Kumar
Networking Research Lab, Department of Electrical/Computer Engineering, The University of Texas-Pan American, Edinburg, USA
Email: sjk@utpa.edu

Received May 15, 2011; revised December 25, 2011; accepted January 30, 2012

ABSTRACT

Cyber attacks are continuing to hamper working of Internet services despite increase in the use of network security systems such as, firewalls and Intrusion protection systems (IPS). Recent Denial of Service (DoS) attack on Independence Day weekend, on July 4th, 2009 launched to debilitate the US and South Korean governments' websites is indicative of the fact that the security systems may not have been adequately deployed to counteract such attacks. IPS is a vital security device which is commonly used as a front line defense mechanism to defend against such DoS attacks. Before deploying a firewall or an IPS device for network protection, in many deployments, the performance of firewalls is seldom evaluated for their effectiveness. Many times, these IPS's can become bottleneck to the network performance and they may not be effective in stopping DoS attacks. In this paper, we intend to drive the point that deploying IPS may not always be effective in stopping harmful effects of DoS attacks. It is important to evaluate the capability of IPS before they are deployed to protect a network or a server against DoS attacks. In this paper, we evaluate performance of a commercial grade IPS Cisco ASA-5510 IPS to measure its effectiveness in stopping a DoS attacks namely TCP-SYN, UDP Flood, Ping Flood and ICMP Land Attacks. This IPS comes with features to counteract and provide security against these attacks. Performance of the IPS is measured under these attacks protection and compared with its performance when these protection features were not available (*i.e*. disabled). It was found that the IPS was unable to provide satisfactory protection despite the availability of the protection features against these flooding attacks. It is important for the network managers to measure the actual capabilities of an IPS system before its deployment to protect critical information infrastructure.

Keywords: Denial of Service (DoS); SYN Flood Attack; Proxy Protection; Firewall Security; Availability

1. Introduction

Exchange of Information in Government organizations, Educational institutions, corporate offices, and for each and every individual mostly depends on Internet. Today everyone, who are using the Internet as media for transferring valuable information, are worrying about securing their systems or networks from attacks on Internet. On August 6th 2009, servers like Twitter, Facebook, Live journal, Google's Blogger and Youtube were under DoS attack, where Twitter was down for several hours [1]. According to "2008 CSI Computer and Security Survey", Firewall type of security technology was used by 94% of the organizations to secure their networks [2]. Many manufacturers are designing firewalls to provide complete protection for their consumers from different types of attacks and at the same time provide availability for good communication between protected private network and public network of the legitimate users. Despite widespread use of firewalls to protect the private networks, the damage caused by the denial of service attacks does not seem to have mitigated. The recent Independence Day Denial of Service attack on July 4th, 2009 launched against US and South Korean government websites [3,4] has caused significant interruption in their operation and now it is prompting many to question the performance of firewalls in defending against such DoS attacks.

In this paper, we evaluate performance of Cisco ASA-5510 Intrusion Prevention System in preventing DDoS attacks. This system provides security to the private networks from many threats on the Internet that already exist and also from the zero day threats. The Denial of Services attacks are over Internet from many years, and there is a lot of research work going on in defending against these attacks. Cisco claims as they are a step forward in defending against these Denials of service attacks. In this paper, we measure the impact of Denial of Service Attack (DoS) on Cisco ASA 5510 Intrusion Prevention System, protecting a Web server (HTTP server) deploying

Windows server 2003. Because of its stateful features, Cisco ASA maintain sessions for each and every packet passing through it. This may cause stateful firewall to consume more resource when compared with a stateless firewall. However it may provide more security than the other techniques [5-9]. Despite of security systems installed to provide security to the private networks, servers have been compromised due to DoS attacks [10-12]. The availability and security provided by the Cisco IPS when it is defending against the DoS attacks explains the performance of the IPS.

The rest of the paper is organized as follows: Section II gives some background about Layer-3 attacks, Ping Flood and ICMP Land Attacks. Section 3 explains the protection techniques used by Netscreen in defending against such attacks. Section 4 explains the Experimental Setup whereas; Section 5 is Results and discussions. Section 6 concludes our findings from this experimental evaluation. Section 7 is Acknowledgments followed by References in Section 8.

2. Dos Attacks

2.1. Layer-4 Denial of Service Attacks

2.1.1. Transmission Control Protocol-SYN Attack

The Transmission Control Protocol (TCP) is a connection oriented protocol. TCP connections are formed between source and the destination hosts before transferring of data. During TCP connection, information is maintained for sockets, sequence numbers and window size. TCP layer provides reliability, flow control, and congestion control, when the connect ion is formed between two hosts. Depending on the Sequence number, Acknowledgment number and the Window size options that are part of TCP header (**Figure 1**). Because of the reason that the connection should be established between unreliable hosts through unreliable Internet, 3-Way Handshake method is used to establish a TCP connection between two applications of the hosts (**Figure 2**).

2.1.1.1 Three-Way Handshake

3-Way Handshake is the connection mechanism used in the Transport Control Protocol. From the **Figure 2**, we can see the connection established between the HTTP client and HTTP server [13]. The process for this connection is given below:

Step 1: Connection was initialized by client, by sending Synchronize Packet (SYN packet) to the server;

Step 2: Server responds to the client by sending SYN_ ACK (Synchronize and Acknowledgment messages);

Step 3: After client receives the SYN_ACK, it replies with final ACK (Acknowledgment message).

When the final ACK is received by the server, the TCP connection is established between the two hosts.

2.1.1.2. Half Open Connections

TCP connections are called Half Open connections when the third step of the 3-Way handshake sending final ACK to the server fails (**Figure 3**), or if one of the hosts closes the connection without acknowledging the other [14]. Half Open connection process is given below:

Step 1: Client initializes the request by sending SYN packet;

Step 2: Server replies to the client with SYN_ACK, and at this point server reserves some resource for the client and waits for the final ACK to arrive (Acknowledgment message);

Step 3: However, the client does not respond to the server with final Ack.

The reason can be that the request initialized by the client could be a spoofed source IP address where that IP address may not exist as the real TCP source.

At this point server waits up to timeout and if it does not receive the final acknowledgment from client, then it releases the resources reserved for the client.

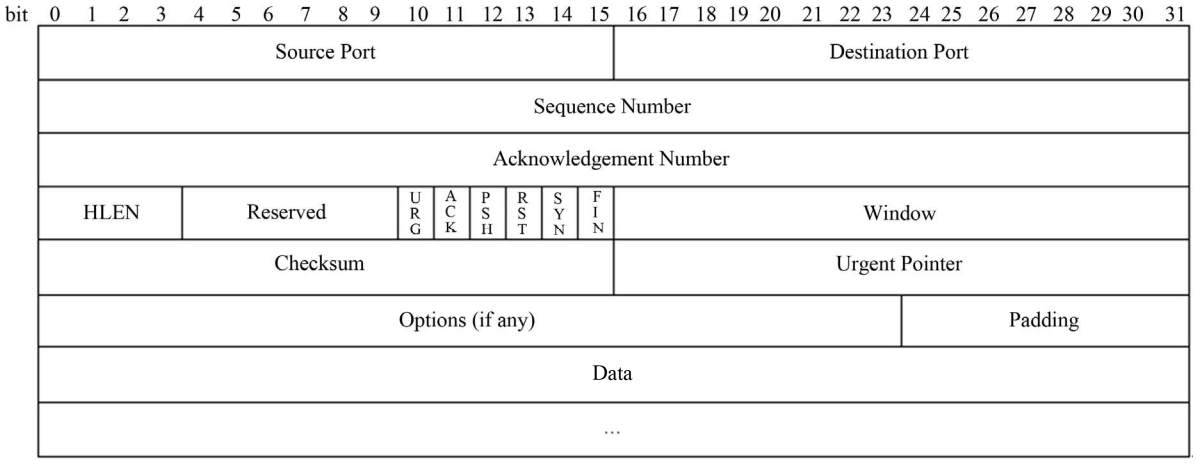


Figure 1. Transmission control protocol.

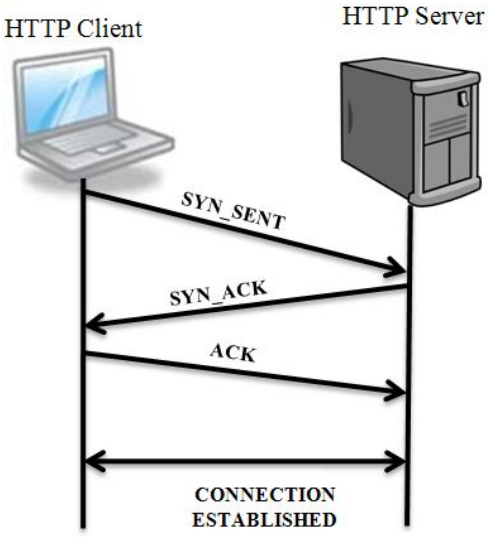


Figure 2. Three-way handshake.

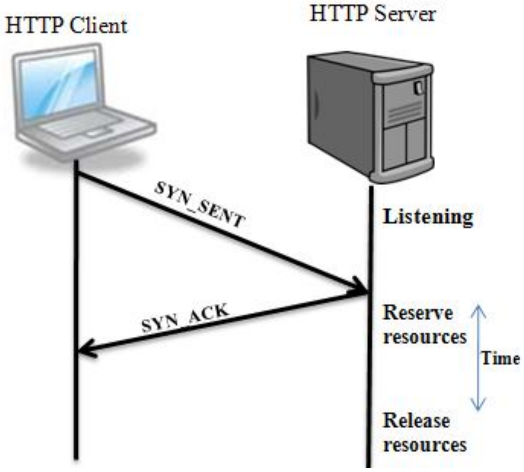


Figure 3. TCP half open connections.

2.1.1.3. TCP SYN Flood Attack

From the **Figure 4**, when the server receives a SYN segment from Internet that was initialized using a spoofed source IP address, it replies to the spoofed IP with a SYN_ACK reserving some resources for the client and waits for final ACK from the client [15]. As the address was a spoofed one, which may not available on Internet temporarily or permanently, the server waits up to time-out and releases the resources.

What happens if the server receives a flood of SYN packets from the Internet with a spoofed source IP address? Resources of the server were consumed totally deceiving the legitimate user from getting the services provided by the server. This Denial of Service attack is called TCP-SYN Flood Attack.

UDP Flood attack is simple, common and famous Layer-4 attack DoS attack. UDP Flood vulnerabilities have been discovered during the year 1998-2000. In this

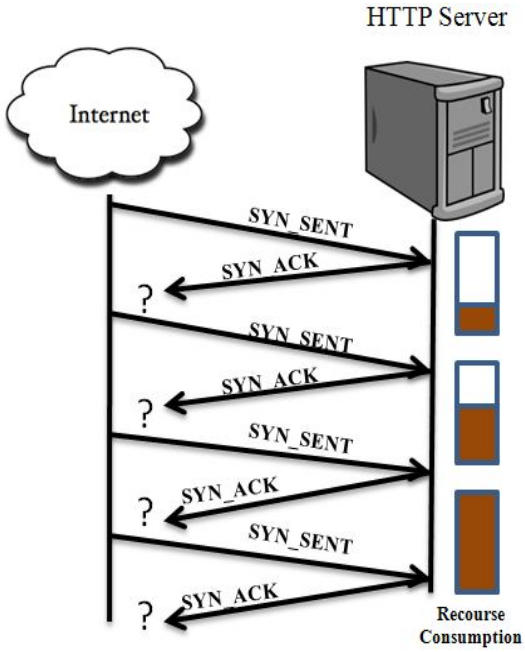


Figure 4. TCP syn flood.

attack a barrage of UDP packets are sent to the victim computer either on selected UDP port or on random port (**Figure 5**). The targeted system processes the incoming datagram to determine which application it has requested on that system by refereeing the port number and in case if the requested application is not present on the system or the requested port was not opened on the targeted system, an ICMP Destination Unreachable message was to the source address from which it receives the datagram, where attackers use spoofed IP address as source address to avoid their identification. If flood of these UDP requests are sent to the targeted system, then it results in Denial of Service attack on the targeted system or the targeted network where victim needs to process all the request and needs to send ICMP Destination Unreachable messages in case if the application was not present on the system, which consumes all the resources of victim [16].

2.2. Internet Control Message Protocol Based Denial of Service attacks

In this DoS attack, attacker takes advantage of ICMP protocol (**Figure 6**) in launching an attack. Internet Control message Protocol (ICMP) is used to diagnose and report any error in a network and which is of Internet Protocol (IP) suit defined in RFC 792 [17]. For example, "Destination Unreachable" is an ICMP message which is generated towards source at the time when the packet is not able to reach the destination, where source can resend the packet to the destination which is a type of error reporting message. "Ping" is an ICMP message used for checking host availability in a network.

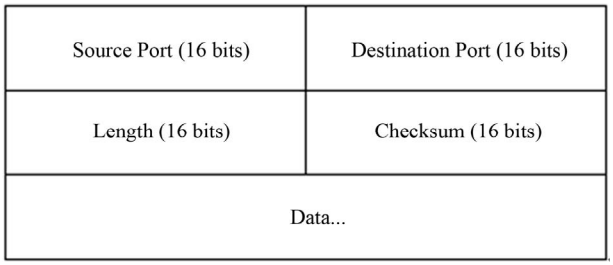


Figure 5. UDP header format.

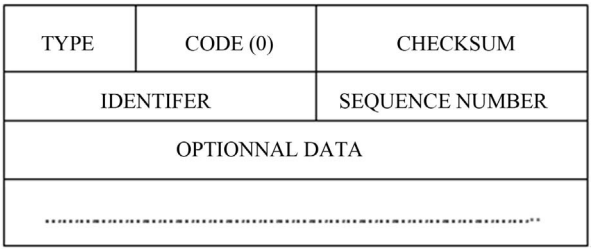


Figure 6. ICMP header format.

ICMP Ping is used by a user to verify the end-to-end Internet path operation, where ICMP Echo Request packet is send to the host and waits for the ICMP Echo Reply packet to confirm that the host is alive in the network [17].

The **Figure 7** shows that host "A" sends the Echo request to host "B" with source address as its own IP address and destination address as host "B" IP address. Then host "B" sends Echo reply confirming host "A" about its presence in the network, by changing the IP address of the source into an echo request as the destination address in the echo reply message. The Type code (**Figure 1**) in Echo Request is 8, and in Echo Reply is 0.

Basing on ICMP, there are so many attacks were ICMP based Ping attack and ICMP based Land attack were used in this thesis.

ICMP Ping DoS Attack

ICMP Ping DoS attack instigate from ping command line which is used to diagnose the network. As DoS attack is flooding illegitimate traffic towards the victim host, in this attack ICMP echo request packet was send towards the victim host and as the host which receives the echo request should reply with the same data to the source host with Echo reply message, the attacker intention is to consume the resources of the victim host. ICMP echo requests when flood towards the victim host, consumes all the resources of the victim in performing the job of sending echo replies for all the echo requests resulted in Denial of Service attack [18,19].

An attacker, by finding the loophole of the network or the Operating system on the victim hosts uses that vulnerability to launch an attack; this will prevents the victim from severing the legitimate users.

ICMP Ping attack is very simple to launch and was the basic of the Denial of Service attacks. And this was also a common type of attack. Victim, who came across this type of attack in a network, thinks that there was some problem in the network, but it was difficult to identify the attack, because attack traffic was similar to the original traffic [18,19].

2.3. ICMP Based Land Attack

ICMP ping is used to sense whether the host is reachable on an IP network or not. However if the host is flooded with continuous Ping Packets with same source and destination IP addresses, result in a DoS attack called ICMP Land Attack [20-23].

When the victim is flooded with continuous ICMP Echo Request having identical source and destination IP address, it needs to reply for the all Echo requests that consumes a lot of resources. As, the echo requests are having source and destination IP address identical, all the Echo replies sent by the victim are received at the victim and eventually dropped, consumes more resources then the earlier as shown in **Figure 8**.

3. Protection Features in Cisco ASA Intrusion Prevention System towards the Denial of Service Attacks

3.1. TCP-SYN Proxy Protection

Layer-4 TCP SYN attack is a well-known DoS attack. Any service that binds to TCP socket is probably vulnerable to TCP SYN flooding attacks. This includes popular web server applications for browsing, file storage and e-mail services on Internet. Protection against this attack is an important for network security.

Cisco ASA provides the SYN-Proxy protection technique to defend the TCP-SYN attack traffic. Maximum connections and maximum embryonic connections are configured, where number is an integer between 0 and 65,535. The default is 0, which means no limit on connections. The following command is used to set the number of connections on the Cisco IOS:

```
hostname(config-pmap-c)#set connection
{[conn-max number] [embryonic-conn-max number]
[per-client-embryonic-max number]
[per-client-max number]
[random-sequence-number {enable | disable}}
```

If the embryonic connection limit reaches, then the Cisco IPS responds to every SYN packet sent to the web server with a SYN-ACK, and does not pass the SYN packet to the internal web server. If the external device responds with an ACK packet, then the security appliance knows it is a valid request. The IPS then establishes

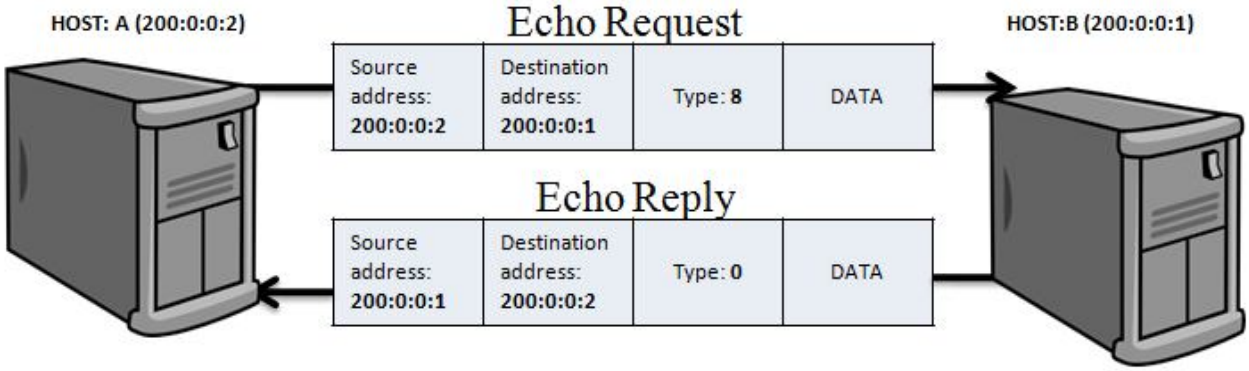


Figure 7. Ping utility.

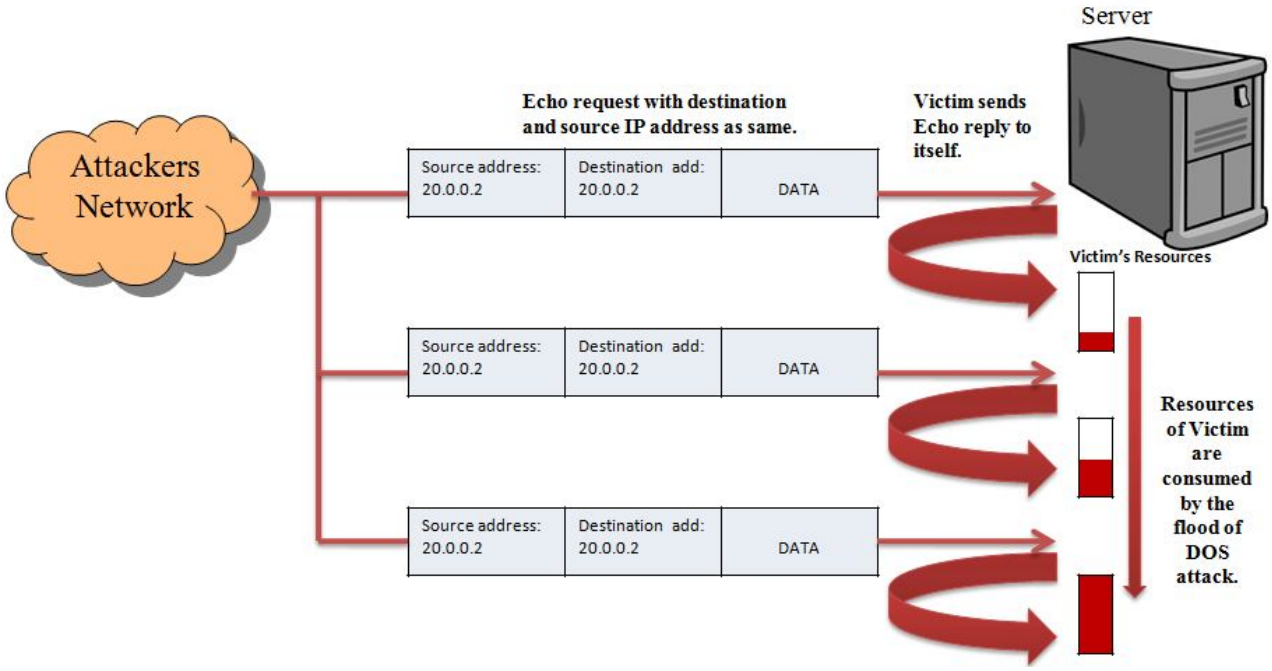


Figure 8. ICMP land attack.

a connection with the web server and joins the connections together. If it does not get an ACK back from the client, it times out that embryonic connection (**Figure 9**).

3.2. UDP Flood Protection

Flood of large number of raw UDP packets targeted at router, firewalls, IPS, IDS and end systems lead to UDP Flood denial of service attack. Many attackers use UDP based attacks, which have a capability to bring the whole network down. This can happen by attacking the Root DNS web servers, which are mainly based on UDP traffic [24-26].

Cisco ASA 5510 has a feature for UDP flood protection, which helps in defending the UDP-flood attacks by setting the threshold limit on the UDP packets. After enableing the UDP flood protection feature, once threshold level is exceeded, it invokes the UDP flood attack protection feature. If the number of UDP datagrams from one or more sources to a single destination exceeds this threshold, the security device ignores further UDP datagrams sent to that destination for the remainder of that second plus the next second as well.

3.3. ICMP Ping Attack Protection

Any IP packet that can be sent across the network can be used to execute a flooding DoS attack. Flood of ICMP echo requests toward the routers, firewalls, Web servers, IPS, IDS and End systems, that are useful for diagnoses, stresses their performance in serving the legitimate users. This stress on the systems due to illegitimate users lead to ICMP Ping flood attack.

Cisco ASA 5510, has inbuilt protection features to

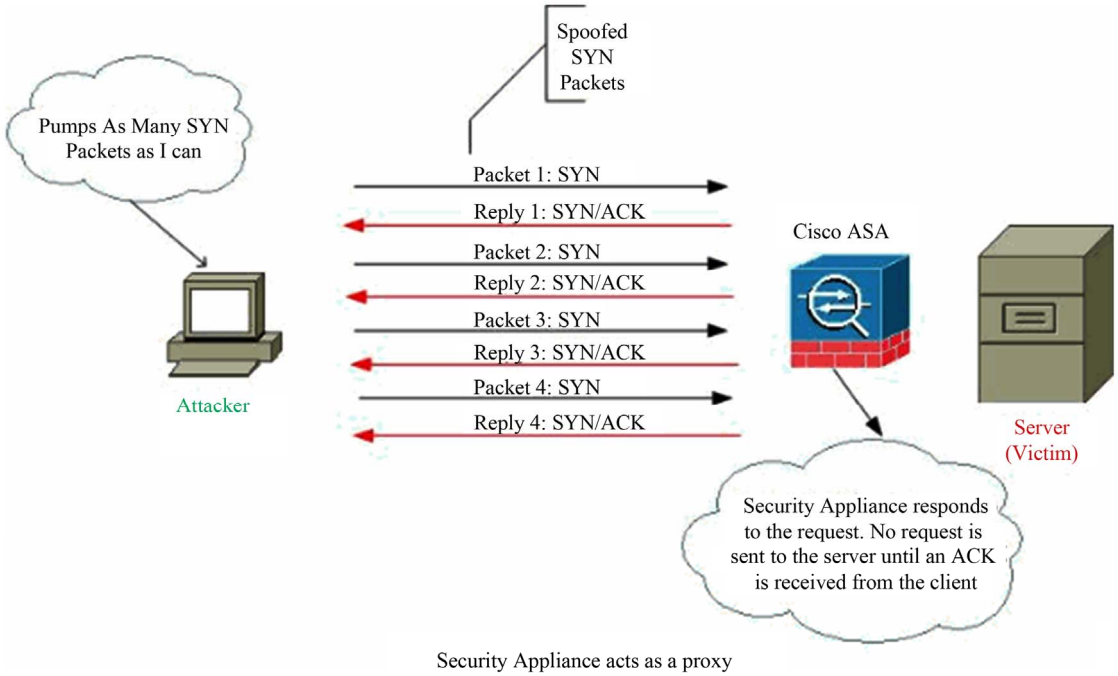


Figure 9. SYN proxy protection in Cisco ASA 5510.

protect against the Layer-3 attacks namely, Ping Flood. When enabling the ICMP flood protection feature in Cisco IPS, one can set a threshold that once exceeded invokes the ICMP flood attack protection feature. If the threshold is exceeded, the Cisco IPS ignores further ICMP echo requests for the remainder of that second plus the next second as well.

3.4. ICMP Land Attack Protection

When the victim is flooded with continuous ICMP Echo Request having identical source and destination IP address, it needs to reply for the all Echo requests that may consumes a lot of resources. As, the echo requests are having source and destination IP address identical, all the echo replies sent by the victim are received at the victim and eventually dropped. This consumes more resources. Flooding a system with such packets can overwhelm the system, causing a denial of service.

On Cisco IPS the Land attack protection was enabled by default, where it blocks the packets with same source and destination IP address as the destination IP address. In Internet, there is no possibility of facing packets with same source and destination IP address. Configuring this protection by default will helps in providing safer communication by preventing illegitimate traffic with spoofed addresses.

4. Experimental Setup

In the Networking Research Lab (NRL) at The University of Texas-Pan American, in a secured network environment we launched different types of DoS attacks on to Cisco ASA-5510. The performance of the in build protection techniques of Cisco ASA in defending the DoS attacks are observed. For this experiment the Cisco ASA—5510 IPS and Windows Web server 2003 on Intel® XeonTM 3 GHz Processor with 4 GB RAM are considered (**Figure 10**).

The maximum number of stable TCP connections that the web server can form with the legitimate users were 20,000 connections per second. The maximum number of stable legitimate TCP connections formed through the Cisco ASA 5510 IPS are 3000 connections per second. In this case, no attack traffic (illegitimate traffic) is sent towards the web server and also there is no protection (allowing all type of connections) configured on the Cisco ASA IPS.

Two cases are compared in each section; one without protection enabled on IPS and other with protection enabled on IPS, for each and every type of DoS attack. When the protection is not enabled on the IPS, it allows all the incoming connections both illegitimate and legitimate traffic. However when the protection on the IPS is enabled, IPS only allows the legitimate traffic and defend the illegitimate traffic.

3000 stable HTTP (TCP-Port 80) successful connections are maintained throughout the test period and attack traffic was applied in the range of 1 Mbps to 100 Mbps towards the web server. While executing the whole process the number of successful connections that are formed with the web server at different loads of attack traffic, amount of attack traffic reaches the web server

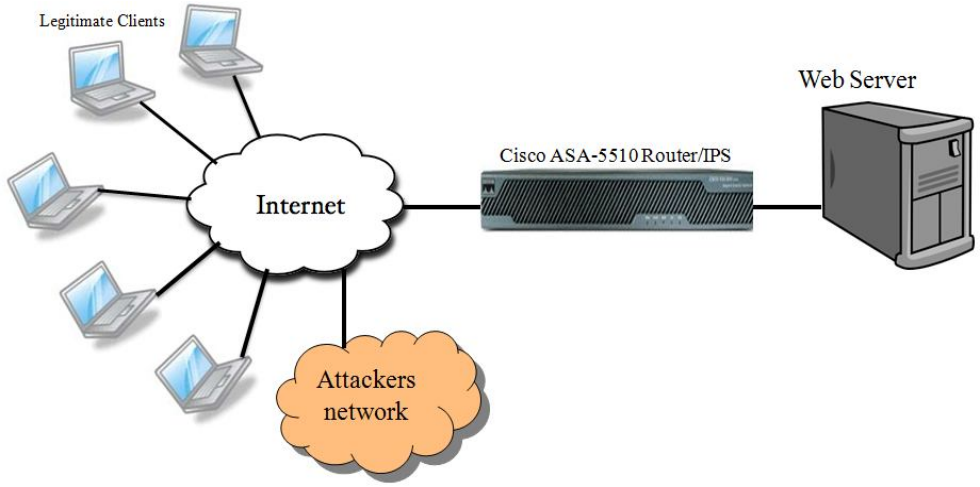


Figure 10. Experimental setup for DoS attacks on web server with Cisco ASA 5510 IPS in between.

and the replies sent by the web server for the corresponding attack load is observed and plotted.

To analyze the results more clearly, before testing the IPS along with the legitimate traffic, the resources consumed by IPS in the absence of legitimate traffic under different attack loads is recorded. These results explain the way the IPS is stressed due to the attack traffic. And these results help us in analyzing the performance of IPS with and without protection in the real time.

Analyzing all these results will help us in providing the defensive capability of Cisco ASA 5510 IPS in defending the common DoS attacks in the Internet.

5. Results and Discussions

5.1. Performance of Cisco ASA 5510 IPS under TCP-SYN Flood Attack

5.1.1. Processor Consumption by IPS under TCP-SYN without Legitimate Traffic

From the **Figures 4** and **3**, it is observed that the processor consumption increases exponentially to 30% at 60 Mbps TCP-SYN attack load and then 50% at 100 Mbps attack load. The exponential increase in the processor consumption along with the attack traffic may lead the legitimate users to denial of service. To observe the effect of this attack load in real time, the results that state the influence of attack on the number of legitimate connections are in the fallow section.

5.1.2. Performance of Cisco IPS under TCP-SYN Attack Along with the Legitimate Connections

From this experiment, it is observed that the legitimate connections are brought down to 66 per second, under TCP-SYN flood attack load of 100 Mbps without protection enabled on the ASA. When the TCP protection was enabled on the ASA it performs better compare to the case when there is no protection. In this case the connections at 100 Mbps TCP-SYN attack load are 1012 per second. When there is no protection on the ASA, at 10 Mbps attack load, successful connections recorded are 2394, and with protection the number improved to 2809. At 60 Mbps attack load, without protection successful connections are brought down to 1103 per second, which is improved by setting the threshold limit for embryonic connections records as 1821 connections per second (**Figure 11**).

The decrease of successful connections can be due to the consumption of resources on the ASA, such as processor, memory or even the bandwidth of the network. By observing the total number of received datagrams by the web server, which are the sum of legitimate packets and the attack packets, the reason behind the decrease in the successful connection rate along with the increase in attack load can be explained.

From **Figures 4** and **5**, it was observed that the number of datagram's received by the web server in the case of no protection on the ASA, are 10,000 per second at 1 Mbps attack load. The datagrams are exponentially increases and reaches to 29,000 at 10 Mbps attack load, and then to the maximum of 77,000 datagrams at 70 Mbps attack load. However at 1 Mbps attack load, the web server is forming 3000 connections per second (**Figure 12**) where 10,000 datagram's per second is recorded. The datagram's increasing with the increase in attack load are attack packets where legitimate packets are less than 10,000 per second. So, without having protection all the attack packets which may initiate the half open connections on the web server by consuming the resources are reaching the web server. Processing all these packets and maintain sessions for all these packets, may consume lot of resources (**Figure 13**).

In case, with the TCP protection enabled on the Cisco ASA, when the attack traffic reaches the threshold limit

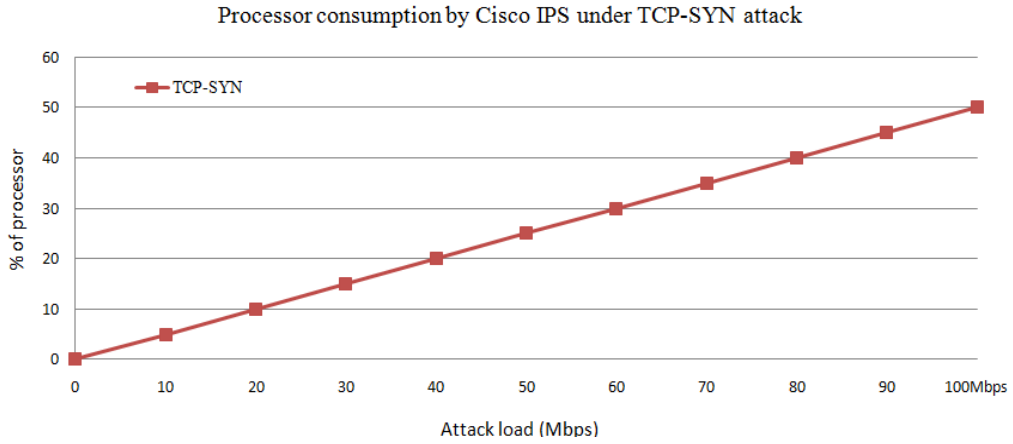
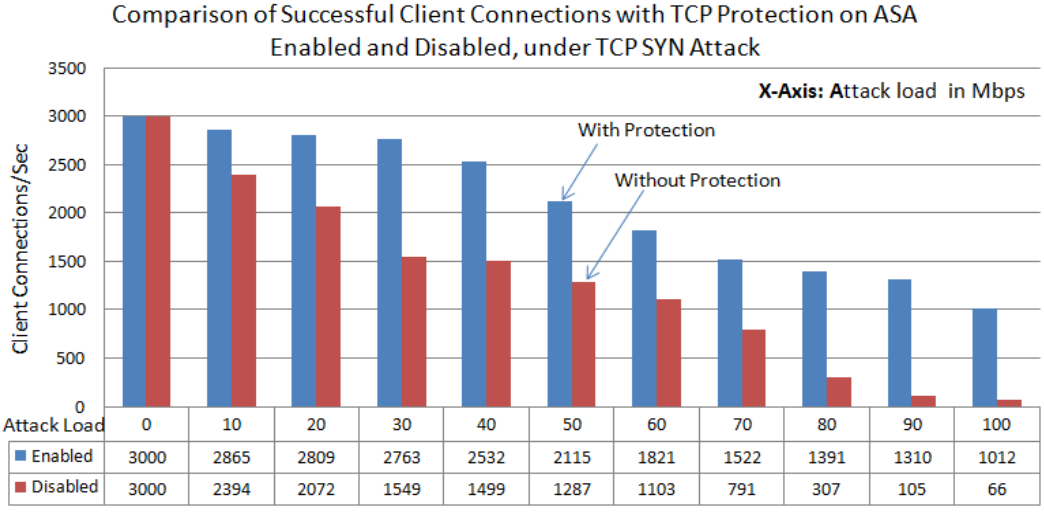


Figure 11. Processor consumption by Cisco IPS under TCP-SYN attack.



Attack Load	0	10	20	30	40	50	60	70	80	90	100
Enabled	3000	2865	2809	2763	2532	2115	1821	1522	1391	1310	1012
Disabled	3000	2394	2072	1549	1499	1287	1103	791	307	105	66

Figure 12. Successful TCP connections formed with web server under TCP-SYN flood attack, at different attack loads, compared at the time of TCP-SYN protection enabled and with the protection disabled the Cisco ASA.

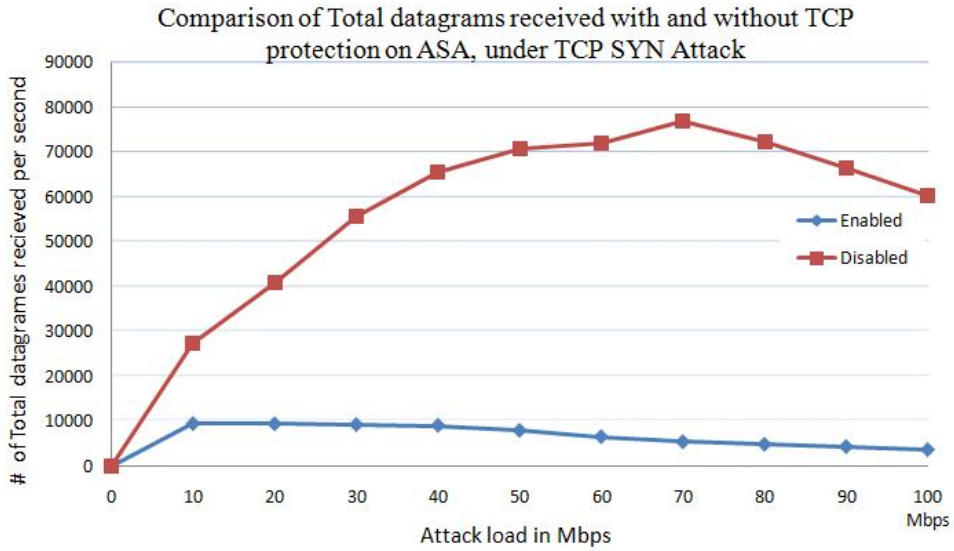


Figure 13. Comparison between total number of datagram's received by the web server at the time of ICMP protection enabled and disabled on the web server.

of 100 half-open connections, then the SYN proxy protection was enabled on the web server. This protection blocks the further SYN packets and acts as proxy. From results, (**Figure 12**) it is observed that only 10,000 datagrams are received by the IPS stably upto 10 Mbps attack load. Then, the received packets are dropped with the increasing of attack load. This explains that, processing the attack packets and protecting the web server by acting as a proxy may consumes resources on the IPS that may leaves limited resources for all the legitimate users. This results in only 1012 connections per second at 100 Mbps attack load.

5.2. Performance of Cisco ASA 5510 IPS under UDP Flood Attack

5.2.1. Processor Consumption by IPS under UDP Flood Attack without Legitimate Traffic

From the **Figure 14**, it is observed that the processor consumption reaches to 96% at 100 Mbps UDP-Flood attack load. It is exponentially increasing, with 65% at 40 Mbps attack load to 85% at 80 Mps attack load. The exponential increase in the processor consumption along with the attack traffic may lead the legitimate users to denial of service.

5.2.2. Performance of Cisco IPS under UDP-Flood Attack Along with the Legitimate Connections

From this experiment (**Figure 15**), it is observed that the legitimate connections are drops to almost zero (less than 50 connections) under UDP flood attack load of 50 Mbps without protection enabled on the ASA. With protection enabled on the ASA, it performs well compare to the case when there is no protection. However in this case the successful connections are brought down to 973 at 100 Mbps attack load. This shows that the protection on the ASA is able to serve better than the case without protection. But still, this protection on the ASA was not able to withstand the higher amounts of UDP Flood attack loads. This results in preventing 70% of the legitimate users from receiving service, from the web server at 100 Mbps attack load (**Figure 15**).

The number of attacks packets received by the web server, number of legitimate traffic received by the web server and also packets sent by the web server in reply to the received packets are observed.

From **Figures 16** and **17**, it is observed that when the UDP protection is not enabled on the ASA, maximum of 140,000 UDP attack packets reach the web server. And web server replies to all the packets received by it with Destination Unreachable messages. On the other hand when the protection is enabled on the ASA, the IPS blocks all the UDP packets that are targeted to bring down the web server and just allows the legitimate traffic. From **Figures 16** and **17**, the number of UDP packets received by the web server at the time of UDP protection enabled are zero. The replies sent by the web server to the received UDP packets are also zero because of this protection.

From **Figure 18**, it is observed that the maximum number of total datagrams received by the web server are 140,000 per second at the time of without protection enabled on it. The total datagram's indicates the sum of legitimate and attack packets. However with the protection enabled it is only 10,000 packets which are only legitimate packets. Processing all the legitimate and attack packets with no protection, and maintaining sessions for all of the packets may consume more resources than the case with protection. Even with dropping the attack packets, in order to provide protection, IPS may consume some resources when a large flood of attack packets reaches the IPS.

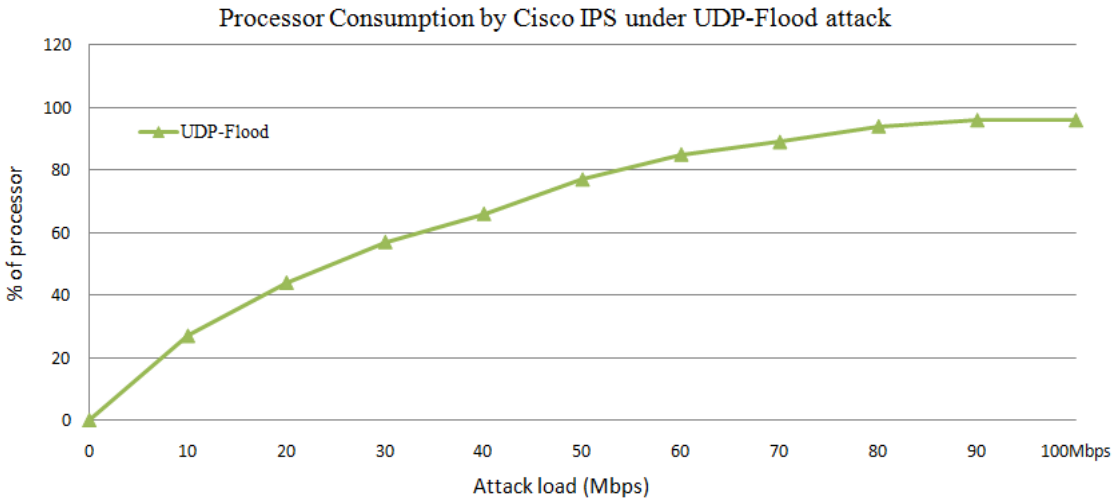
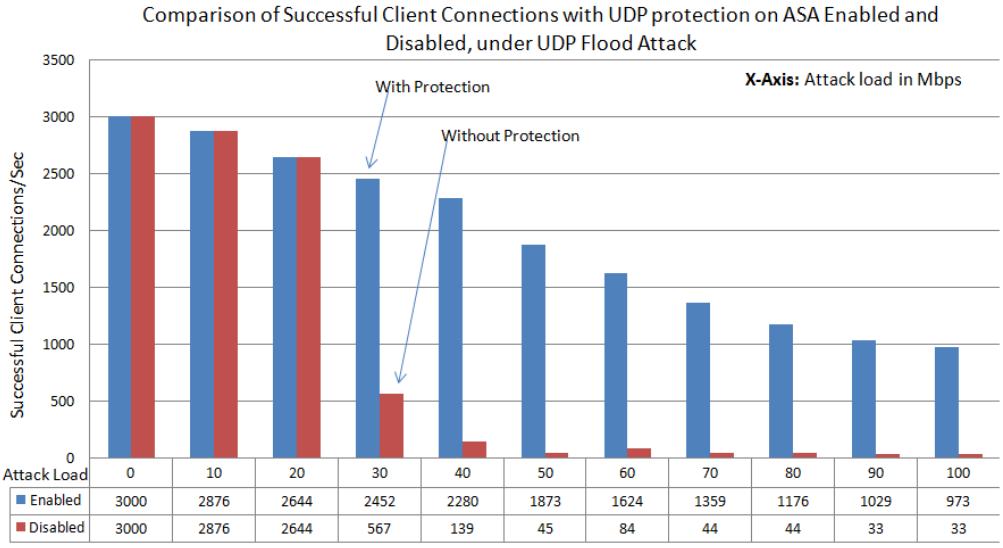


Figure 14. Processor consumption by Cisco IPS under UDP flood attack.



Attack Load	0	10	20	30	40	50	60	70	80	90	100
Enabled	3000	2876	2644	2452	2280	1873	1624	1359	1176	1029	973
Disabled	3000	2876	2644	567	139	45	84	44	44	33	33

Figure 15. Successful TCP connections formed with web server under UDP flood attack, at different attack loads, compared at the time of UDP security enabled with UDP security disabled on the Cisco ASA.

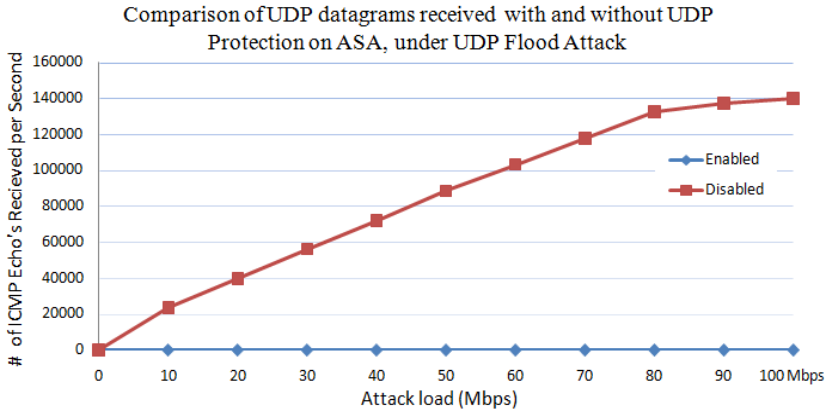


Figure 16. Comparison of UDP datagrams received by web server at the time of UDP flood protection enabled and disabled on the Cisco ASA.

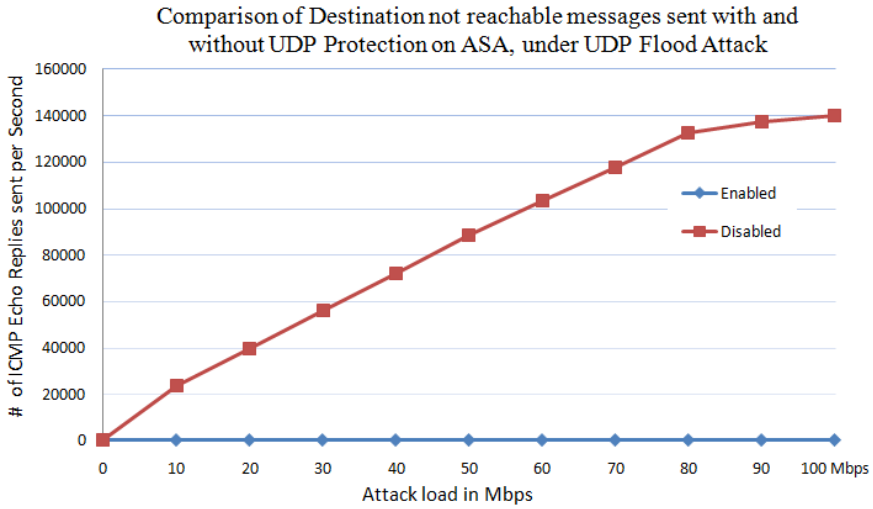


Figure 17. Comparison of Destination not reachable messages sent by web server at the time of UDP flood protection enabled and disabled on Cisco ASA.

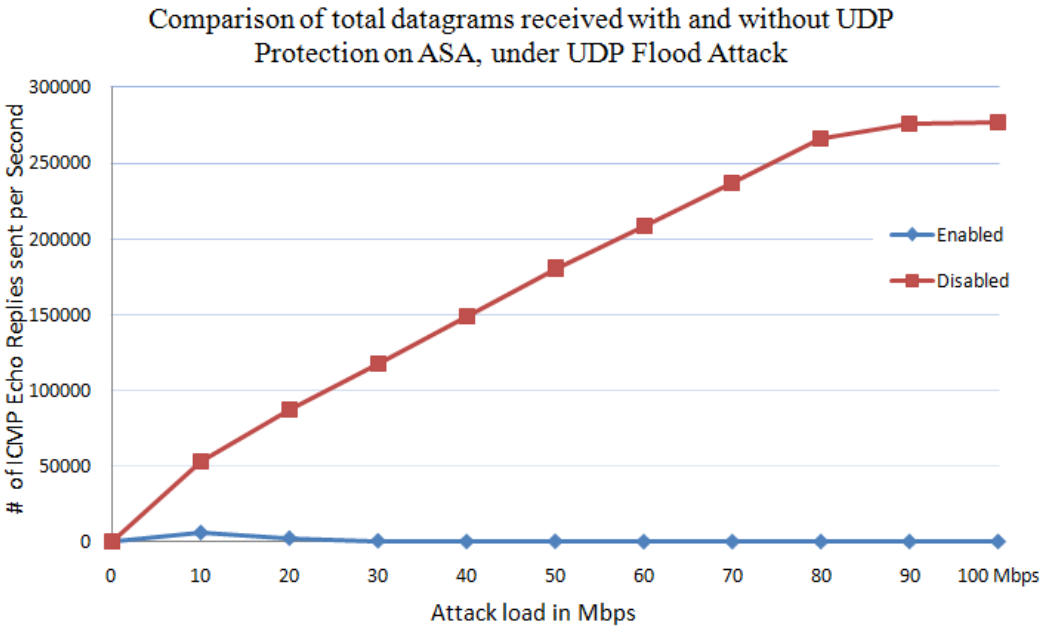


Figure 18. Comparison between total number of datagrams received by the web server at the time of ICMP protection enabled and disabled on the web server.

5.3. Performance of Cisco ASA 5510 IPS under ICMP PING Attack

5.3.1. Processor Consumption by IPS under ICMP-PING Attack without Legitimate Traffic

From the **Figure 19**, it is observed that the processor consumption reaches to 97% at 30 Mbps Ping attack load. The processor consumption of 97% by the attack traffic may lead the legitimate traffic to denial of service. To observe the effect of this attack load in real time, the influence of attack traffic on the performance of Cisco IPS is observed under stable simulated legitimate users.

5.3.2. Performance of Cisco IPS under ICMP-PING Attack Along with the Legitimate Connections

From these results (**Figure 20**), it is observed that the legitimate connections are brought down to almost zero (less than 30 connections) under ICMP Ping flood attack at attack load of 20 Mbps without protection enabled on the ASA. At the time when the protection is enabled on the ASA, it is performing better compare to the case when there is no protection. However in this case, the successful connections drops to 176 connections at 40 Mbps attack load. And at 90 Mbps attack load the successful connections are almost drops to zero. This shows that, the protection on the ASA was able to serve better than the case without protection but still this protection on the ASA was not able to withstand the higher amounts of ICMP Ping flood attack load. This still results in denial of service preventing the illegitimate users from getting service from the web server (**Figure 20**).

The decrease of successful connections can be due to the consumption of resources on the ASA, such as processor, memory or even the bandwidth of the network. These may cause the ASA to drop the legitimate users or even take more time to process the packets. The number of attack packets (Illegitimate packets) received by the web server.

From **Figures 21** and **22**, it is observed that when the ICMP protection is disabled on the ASA, maximum of 10,500 ICMP attack packets (Echo's) reaches the web server. Web server replies to all the ICMP packets received by it with echo replies. On the other hand, when the protection is enabled on the Cisco IPS, the IPS blocks all the ICMP packets that are sent to bring down the web server and just allows the legitimate traffic. So, it is observed from the **Figures 21** and **22**, the number of ICMP packets received by the web server at the time of security enable are zero. So the replies sent by the web server to the received echo's are also zero.

From **Figure 23**, it is observed that the number of total datagrams received by the web server are stable after 20 Mbps attack load at 11,000 connections per second without ICMP protection. However from **Figure 21**, the total ICMP echo's received by the web server, which are attack packets, are around 10,500 after 20 Mbps of attack load. This explains that the packets reaching the serve after the 20 Mbps of attack traffic is only the attack traffic. In case with protection enable, the total number of datagram's received by the web server decreases with increase in the attack load. And all the datagram's received by the web server are only legitimate packets, which are brought down rapidly with increase in the attack load.

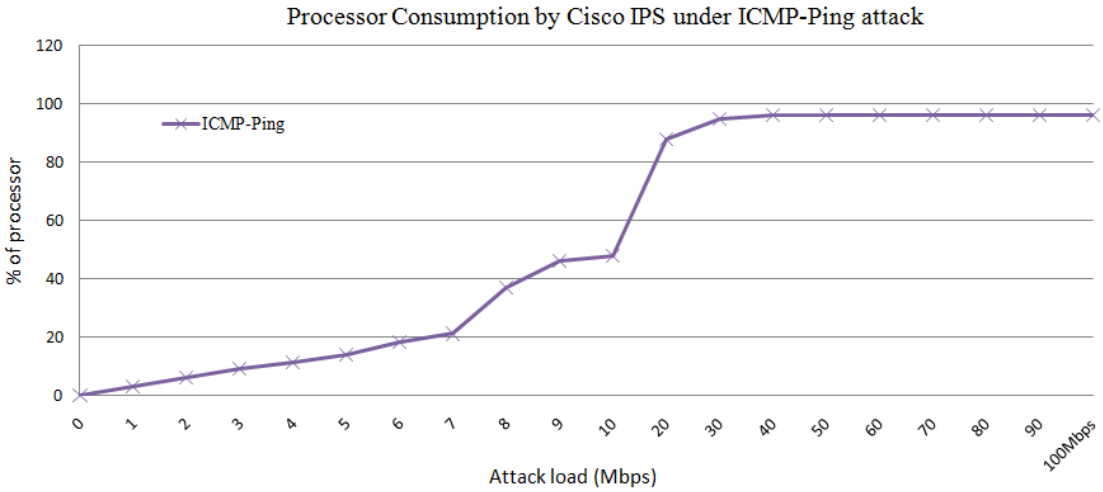
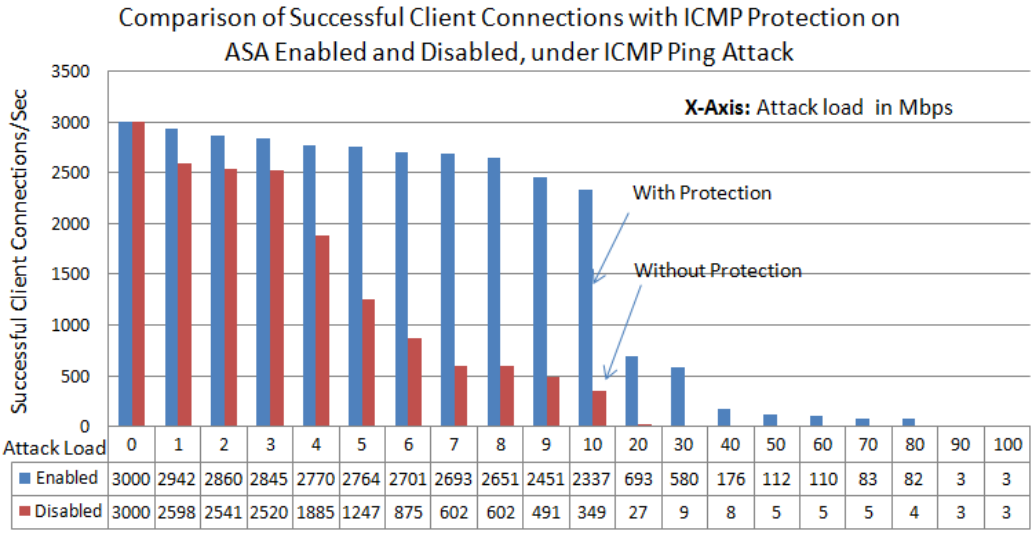


Figure 19. Processor consumption by Cisco IPS under ICMP ping attack.



Attack Load	0	1	2	3	4	5	6	7	8	9	10	20	30	40	50	60	70	80	90	100
Enabled	3000	2942	2860	2845	2770	2764	2701	2693	2651	2451	2337	693	580	176	112	110	83	82	3	3
Disabled	3000	2598	2541	2520	1885	1247	875	602	602	491	349	27	9	8	5	5	5	4	3	3

Figure 20. Successful TCP connections formed with web server under ICMP ping flood attack, at different attack loads, compared at the time of ICMP security enabled and disabled on the Cisco ASA.

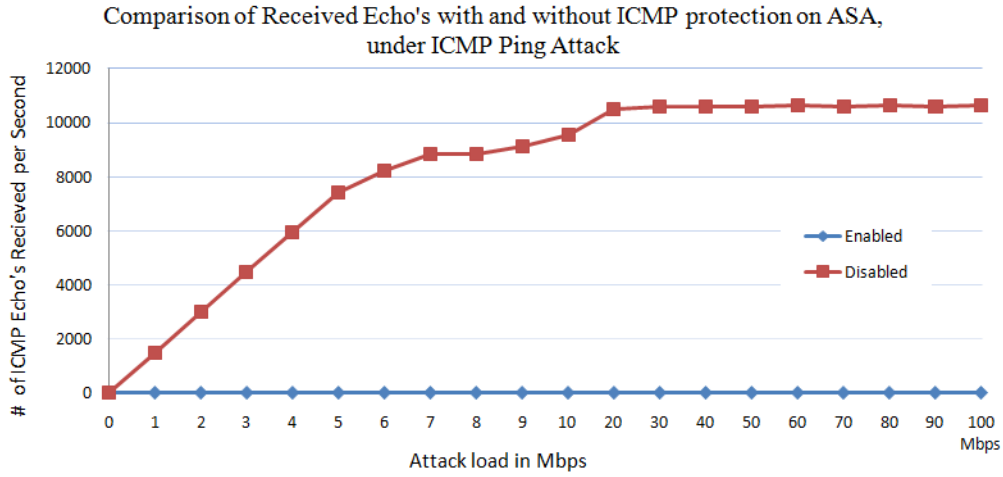


Figure 21. Number of ICMP echo's requests received by the web server with and without of ICMP protection on the Cisco ASA-IPS.

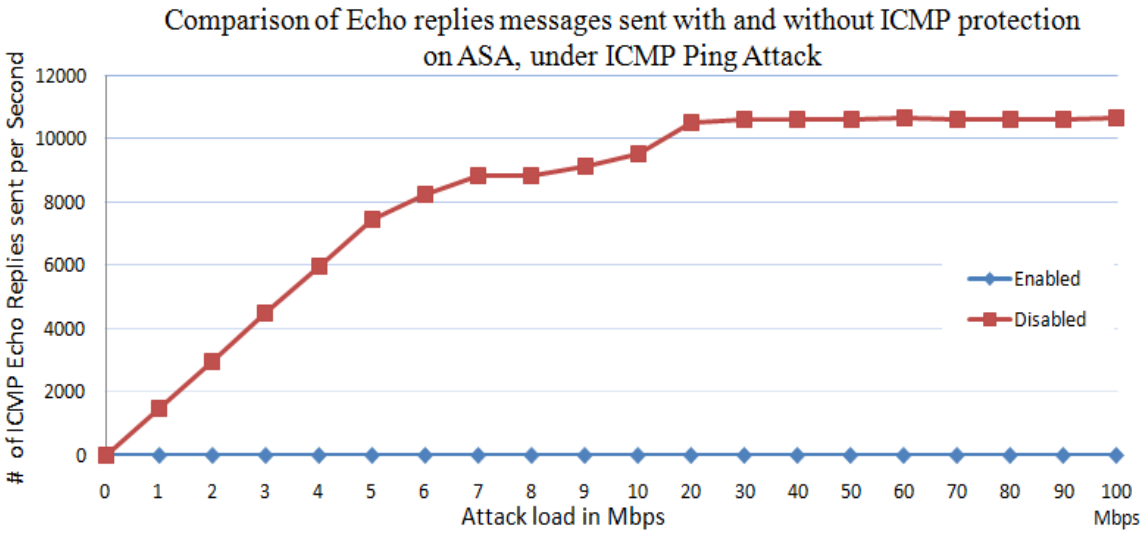


Figure 22. Number of ICMP echo's replies sent by the web server with and without of ICMP protection on the Cisco ASA-IPS.

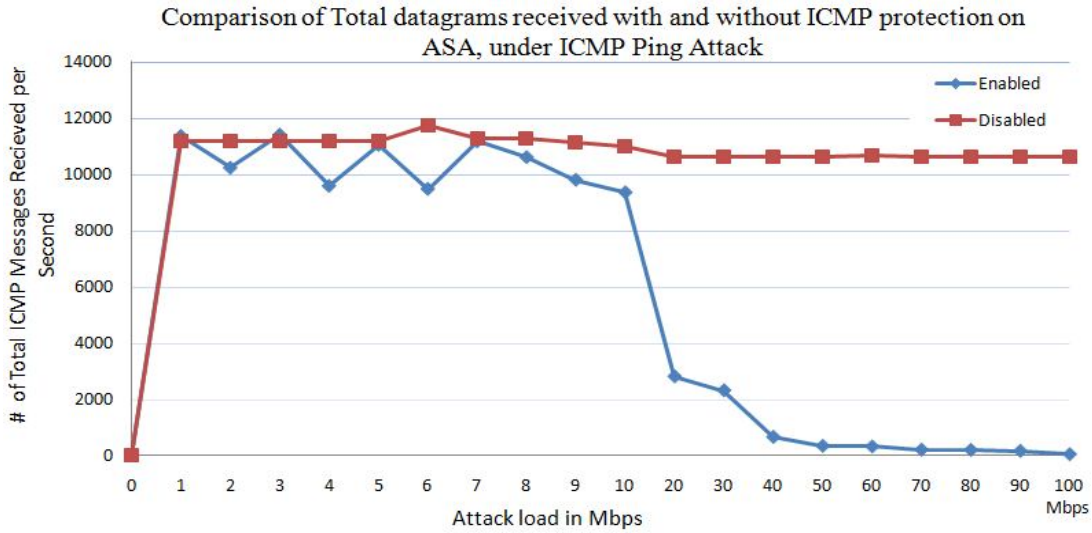


Figure 23. Total number of datagrams received by the web server with and without ICMP protection enabled on Cisco IPS.

5.4. Performance of Cisco ASA 5510 IPS under ICMP Land Attack

5.4.1. Processor Consumption by IPS under Land Attack without Legitimate Traffic

From **Figure 24**, it is observed that the processor consumption reaches to 97% at 30 Mbps Land attack load. The processor consumption of 97% by the attack traffic may lead the legitimate users to denial of service. To observe the effect of this attack load in real time, the influence of attack traffic on the performance of Cisco IPS is observed under stable simulated legitimate users.

5.4.2. Performance of Cisco IPS under ICMP-Land Attack Along with the Legitimate Connections

From this experiment (**Figure 25**), it is observed that the legitimate connections are brought down to 700 under ICMP Land attack load of 40 Mbps with default Land Attack protection enabled on the ASA. The number of connections are brought down to 633 at land attack load of 60 Mbps, and at 100 Mbps attack load total connections are 177 per second. This shows that the Land attack protection on the ASA was not able to withstand the higher amounts of ICMP Land DoS attack load. This results in preventing the maximum number of legitimate users from getting service, from the web server.

Successful TCP Connections formed with web server under ICMP Land attack, at different attack loads, with ICMP Land attack security enabled by default on the Cisco ASA.

The number of attack packets and legitimate packets received by the web server and also the packets sent by the web server in reply to the received packets are observed. It is observed that the default ICMP Land Attack

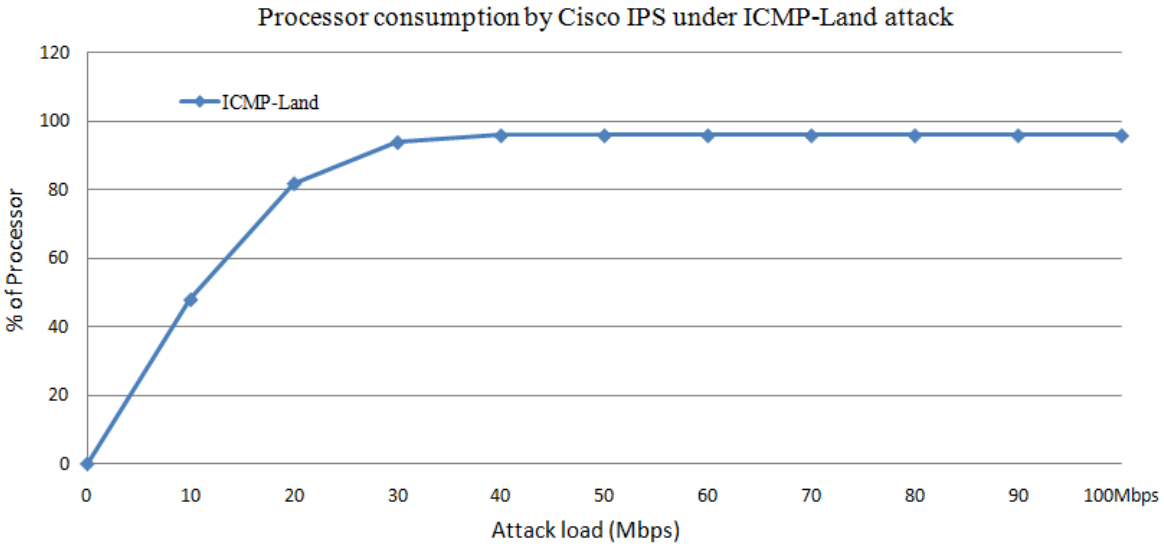


Figure 24. Processor consumption by Cisco IPS under ICMP land attack.

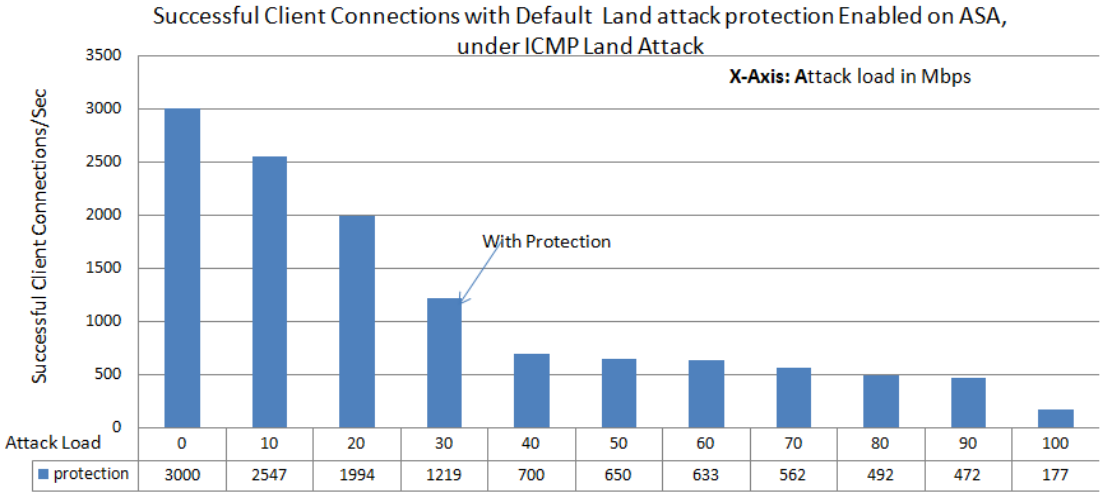


Figure 25. Successful TCP Connections formed with web server under ICMP land attack, at different attack loads, with ICMP Land attack security enabled by default on the Cisco ASA.

protection enabled on the ASA blocks all the Land attack packets which are having the source and destination IP addresses, same as the targeted victim address. On the web server, no ICMP Echo packets are received and no Echo replies are sent by the web server.

From **Figure 26**, it is observed that the number of total datagrams received by the web server are almost 12,000 per second upto the 20 Mbps of Land attack load, with the default ICMP Land attack protection enabled on the Cisco IPS. As, the total attack packets received by the web server are zero, which explains that the packets reaching the web server are only legitimates packets (TCP-Segments). The total datagram's received by the web server from 40 Mbps of attack load are 200 datagrams per second, is may be due to the resources consumed by the Land attack packets. Where Cisco ASA needs to processes the received land attack packets and then drop them when if finds them as land attack traffic. Dropping the land attack packets helps in not allowing the land attack traffic reaching the web server and consuming resources on the web server. However processing such a huge amount of packets and allowing the legitimate traffic at the same time left the IPS with limited resources (**Figure 24**) for the legitimate traffic. This lead to no service for most of the clients, after reaching 40 Mbps attack traffic (**Figure 25**).

6. Conclusions

The evaluation of popular Cisco ASA-5510 intrusion prevention system, which is a latest technology and has built in security features for Denial of Service attacks. This was stressed under DoS attacks and the performance

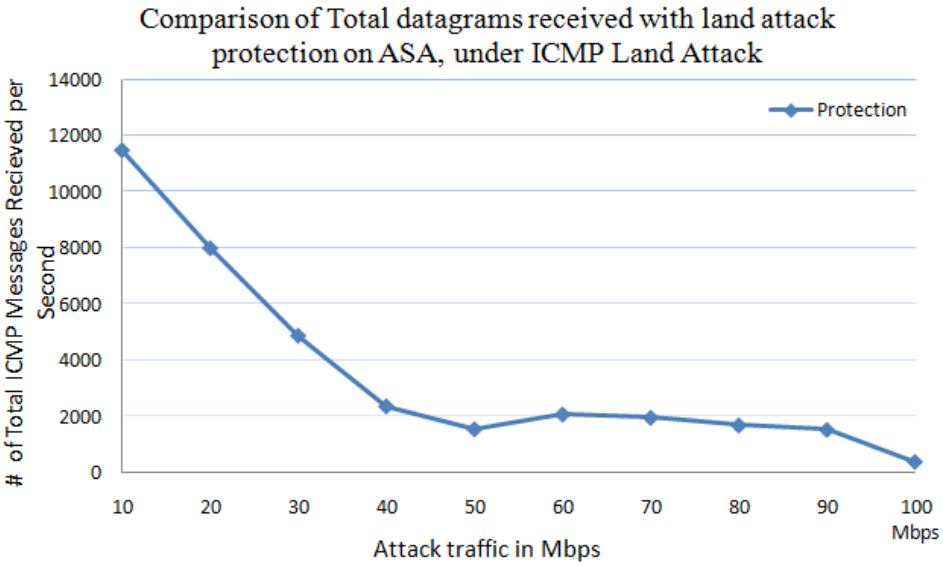


Figure 26. Comparison between total number of datagrams received by the web server at the time of ICMP protection enabled and disabled on the web server.

in defending them was observed in the paper. As Cisco is one of the leading manufacturers in security systems we selected this for our experiments. It was tested against DoS attacks such as TCP-SYN Flood, ICMP-Ping Flood, ICMP-Land and UDP-Flood attacks. The IPS is used to secure the Web server installed on Windows web server 2003. The maximum number of successful stable TCP connection rate formed with the web server was 3000 per second. We had two cases for each type of DoS attack traffic, with the protection on ASA enabled and disabled.

When the ICMP-Ping flood attack was sent towards the web server through IPS, without any protection enabled on the IPS, it was observed as almost zero connections at 20 Mbps attack load. And at 10 Mbps attack load 349 successful connections were observed and at low amount of 5 Mbps attack load the connections were brought down to 1247 per second. However, with ICMP protection enabled on the IPS, it resulted in 2337 connections at 10 Mbps attack load. And at 90 Mbps attack load the connections drops to zero. This shows improvement with the protection on the IPS, but after 40 Mbps attack load, no legitimate users were able to use the services. In the case of Land attack, Cisco ASA has the protection by default, because of the attack packets structure. The packets with same source and destination IP addresses were identified as land attack packets and were blocked. Under this attack, the connections were recorded as 1219 at attack load of 30 Mbps and at 90 Mbps it was recorded as 472 connections per second. This may be due to the overhead created by the land attack packets on the IPS in processing those packets and verifying with the default security features. This may utilizes more resources at higher attack loads. Under TCP-SYN attack without protection, the connections were brought down to 50% of the total legitimate connections at attack load of 40 Mbps, and at 80 Mbps attack load, it was recorded as less than 307 connections. However by enabling SYN protection with threshold limit for embryonic connections as 100, there was an improvement in the number of connections. At 40 Mbps the recorded connections were 2500 and at 80 Mbps they were 1300. Under UDP flood attack without protection, the number of successful connections were around 500. And with protection it was improved to around 2500. At 90 Mbps UDP flood attack traffic without protection, the connections observed were 33, with protection this was improved to 1000 connections per second.

REFERENCES

[1] CNET News, "Twitter Crippled by Denial-of-Service Attack," 2009. http://news.cnet.com/8301-13577_3-10304633-36.html

[2] R. Richardson and CSI Diretor, "2008 CSI Computer Crime & Security Survey," SCI, 2008.

[3] IBN Live World, "US Suspects N Korea Launched Internet Attack," 2009. http://ibnlive.in.com/news/us-suspects-n-korea-launched-internetattack-on-%20%20%20%20%20july-4/96715-2.html

[4] R. S. R. Gade, A. S. S, Leonel and S. Kumar, "Are Microsoft Windows Servers' Capable of Defending against Security Attacks?" *Poster Presentation of HESTEC Science Symposium*, The University of Texas-Pan American, Edinburg, 2010.

[5] "Defeating DDoS Attacks," 2010. http://www.ciscosystems.net/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/prod_white_paper0900aecd8011e927.html

[6] "Strategies to Protect against Distributed Denial of Ser-

vice (DDoS) Attacks," 2010. http://www.cisco.com/en/US/tech/tk59/technologies_white_paper09186a0080174a5b.shtml

[7] "DDoS Protection Solution Builds on Cisco Managed Service Leadership," 2010. http://newsroom.cisco.com/dlls/2005/prod_060605b.html

[8] "Using CAR during DOS Attacks," 2010. http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a00800fb50a.shtml

[9] Cisco Visual Networking Index Forecast, "Ascending the Managed Services Value Chain," 2008. http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns546/white_paper_c11-5540

[10] R. Richardson, "2008 CSI Computer Crime and Security Survey," 2008. http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

[11] The FBI Federal Bureau of Investigation, "Mafiaboy Pleads Guilty," 2010. http://www.fbi.gov/pressrel/pressrel01/mafiaboy.htm

[12] "FBI Ranks Cyber Attacks Third Most Dangerous behind Nuclear War and Weapons of Mass Destructions," 2010. http://www.tgdaily.com/security-features/40861-fbi-ranks-cyber-attacks-third-most-dangerous-behind-nuclear-war-and-wmds

[13] S. Kumar and E. Petana, "Mitigation of TCP-SYN Attacks with Microsoft's Windows XP Service Pack2 (SP2) Software," *Proceedings of the 7th International Conference on Networking of IEEE*, New York, 13-18 April 2008. doi:10.1109/ICN.2008.77

[14] P.-E. Liu and Z.-H. Sheng, "Defending against TCP SYN Flooding with a New Kind of SYN-Agent," *Proceedings of the* 2008 *International Conference on Machine Learning and Cybernetics*, Kunming, 12-15 July 2008, pp. 1218-1221. doi:10.1109/ICMLC.2008.4620589

[15] R. K. C. Chang, "Defending against Flood-Based Distributed Denial-of-Service Attack: A Tutorial," *IEEE Transactions on Communication Magazine*, Vol. 40, No. 10, 2002, pp. 42-51. doi:10.1109/MCOM.2002.1039856

[16] W. Chen, D.-Y. Yeung and P.-E. Liu, "Defending against TCP SYN Flooding Attacks under Different Types of IP Spoofing," *Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies*, (*ICN*/*ICONS*/*MCL* 2006), Wuhan, 23-29 April 2006, p. 38. doi:10.1109/ICNICONSMCL.2006.72

[17] J. Postel, "Internet Control Message Protocol," 2010. http://www.faqs.org/rfcs/rfc792.html

[18] S. Sirisha and S. Kumar, "Is McAfee SecurityCenter/Firewall Software Providing Complete Security for Your Computer?" *Proceedings of the International Conference on Digital Society of the IEEE ICDS*, St. Maarten, 10-16 February 2010, pp. 178-181. doi:10.1109/ICDS.2010.38

[19] S. Kumar, "PING Attack—How Bad Is It?" *Computers & Security Journal*, Vol. 25, No. 5, 2006, pp. 332-337. doi:10.1016/j.cose.2005.11.004

[20] R. S. R. Gade, H. Vellalacheruvu and S. Kumar, "Performance of Windows XP, Windows Vista and Apple's Leopard Computers under a Denial of Service Attack," *Proceedings of the* 4*th International Conference on Digital Society of the IEEE ICDS*, St. Maarten, 10-16 February 2010, pp. 188-191. doi:10.1109/ICDS.2010.39

[21] R. S. R. Gade, S. Sirisha, H. Vellalacheruvu and S. Kumar, "Impact of Land attack Compared for Windows XP, Vista and Apple's Leopard," *Poster Presentation of the HESTEC Science Symposium*, The University of Texas-Pan American, Edinburg, 2009.

[22] S. Kumar, *et al*., "Can Microsoft's Service Pack2 (SP2) Security Software Prevents Smurf Attacks?" *Proceedings of the International Conference on Internet and Web Applications and Services*/*Advanced International Conference on Telecommunications of the IEEE AICT-ICIW*'06, 19-25 February 2006, p. 89. doi:10.1109/AICT-ICIW.2006.60

[23] S. Kumar, "Smurf-Based Distributed Denial of Service (DDoS) Attack Amplification in Internet," *Proceedings of the* 2*nd International Conference on Internet Monitoring and Protection of the IEEE ICIMP* 2007, San Jose, 1-5 July 2007, p. 25. doi:10.1109/ICIMP.2007.42

[24] D. K. Y. Yau, J. C. S. Lui, L. Feng, and Y. Yeung, "Defending against Distributed Denial of Service Attacks with Max-Min Fair Server-Centric Router Throttles," *Journal of IEEE*/*ACM Transactions on Networking*, Vol. 13, No. 1, 2005, pp. 29-42. doi:10.1109/TNET.2004.842221

[25] R. K. C. Chang, "Defending against Flood-Based Distributed Denial-of-Service Attack: A Tutorial," *IEEE Transactions on Communication Magazine*, Vol. 40, No. 10, 2002, pp. 42-51. doi:10.1109/MCOM.2002.1039856

[26] Y. Xu, "Statistically Countering Denial of Service Attacks," *Proceedings of the International Conference on Communications of the IEEE ICC* 2005, Seoul, 16-20 May 2005, pp. 844-849. doi:10.1109/ICC.2005.1494470

