12-2010

# Experimental evaluation of select servers and firewalls under denial of service security attacks

Raja Sekhar Reddy Gade
*University of Texas-Pan American*

# EXPERIMENTAL EVALUATION OF SELECT SERVERS AND FIREWALLS UNDER DENIAL OF SERVICE SECURITY ATTACKS

A Thesis

by

RAJA SEKHAR REDDY GADE

Submitted to the Graduate School of the
University of Texas-Pan American
In partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

December 2010

Major Subject: Electrical Engineering

# EXPERIMENTAL EVALUATION OF SELECT SERVERS AND FIREWALLS UNDER DENIAL OF SERVICE SECURITY ATTACKS

A Thesis

by

RAJA SEKHAR REDDY GADE

COMMITTEE MEMBERS

Dr. Sanjeev Kumar
Chair of Committee

Dr. Weidong Kuang
Committee Member

Dr. Jaime Ramos
Committee Member

December 2010

ABSTRACT

Gade, Raja Sekhar Reddy, Experimental Evaluation of Select Servers and Firewalls under Denial of Service Security Attacks. Master of Science (MS), December, 2010, 130 pp., 82 figures, 79 references.

Internet security requires newer prevention mechanisms to be implemented on web-servers and routers. Firewall/Intrusion Prevention mechanisms (IPS) can be deployed on host servers or routers as an added line of defense against Internet attacks. In this thesis, we evaluate performance of security mechanisms provided by these devices against Distributed Denial of Service (DDoS) attacks. The host based firewalls on Windows servers-2003 and 2008 were evaluated. In this thesis, we also evaluated Juniper Networks Netscreen-5GT firewall/IPS, and Cisco ASA-5510/IPS that are used in protecting web-servers against DDoS attacks. It was found that the host based firewalls and protection mechanisms on the windows servers were not capable of defending against the DDoS attacks. Our performance evaluation showed the computing resource of the servers to be completely exhausted under these attacks. The evaluation of firewalls and IPS under different loads of attack had varying performance in supporting the number of web connections.

# DEDICATION

The completion of my master studies would not have been possible without the blessings and divine support of GOD. I would like to dedicate my work to my parents, Shri Venkata Reddy Gade and Smt. Naga Malleswari Gade for their love and exceptional support, to my grandfather Shri Venkata Subha Reddy Gade and to my favorite politician Dr. Y. S. Raja Sekhar Reddy. This thesis would be incomplete without love, affection and caring of my lovely family members and cool friends.

# ACKNOWLEDGMENTS

I would like to formally thank:

Dr.Sanjeev Kumar, my Advisor and Committee Chair, for his profound help and belief in my abilities. Without you this Thesis would have not been possible. Thank you so much for your entire support and encouragement.

Dr. Weidong Kuang and Dr. Jaime Ramos for their willingness to serve as committee members. Thank you for your support and guidance.

My fellow Graduate students in the NRL lab; Hari, Sirisha, Abhi and Leo for the technical discussions and knowledge sharing. Thank you so much for your support.

All my friends kalyan, Pavan, Varma, Joy, Bharath, Teja, Sumanth, Rama, Nani; My loved ones Nagama akka, Bava, Seshi Reddy Padhanana, Ammu, Rani, Naresh, , and rest of my family. Thank you all for your love and affection.

Work in this thesis is supported in part by the grant awarded to Dr. Kumar by the National Science Foundation (NSF) under Grant No. 0521585.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

# CHAPTER I

## INTRODUCTION

Internet transformed the Global communications at large by connecting people across the world. Today exchange of valuable information in Government Organizations, Educational institutions, corporate offices or each and every individual is widely dependent on Internet. Over the years, Internet has been expanded into many fields and million dollar businesses are using it as a medium of communication.

Internet is expanding rapidly in all the fields:

- In education, it makes research available online where information is able to share quickly.
- In communication there are Electronic mails and chats, which decrease the complexity in communication from different places of the world.
- In medical field introducing remote surgery (Telesurgery), develops the availability of good health care to the corners of the world with less complexity and time.
- In government functions, it helps in maintaining confidential and fast communication.
- In commercial sector like banking, shopping, and insurance makes things more flexible and affordable.
- And also in entertainment, maintaining blogs, social communities by sharing views of people throughout the world.

Technically, Internet is a collection of networks, where users store and share information with servers between them. The information transferred/shared between networks in Wide Area Network (WAN) or Local Area Network (LAN) is processed by Routers and Switches. Internet has disadvantages, coined with great advantages. There are many security problems over Internet, from the time it evolved. To maintain secure communication over Internet, security systems are placed at the entrance of the trusted network (Private Network). Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), and Firewalls are the security systems used to protect against security threats over Internet.

The threats over Internet are increasing at a very rapid pace. To prevent against threats, many new techniques have been discovered and implemented. These developments lead to the era of intelligent routers and switches. Where, Firewall and Intrusion Prevention mechanisms (IPS) can be deployed on routers as an added line of defense against Internet attacks. End systems with different Operating Systems are also equipped with built-in protection techniques. However third party security software's for end systems are also available in the markets.

Inspite of all the available security systems, attacks on the servers owned and maintained by the US government and also popular websites which were believed under world's heavily secured environment are facing problems over Internet [1-4]. Bringing down these servers may cause great damage to the public (users). The reason behind this is, everyone knows about the virus, worms but there is no much awareness about Denial of service attacks. DoS attacks born along with virus and worms. Virus and Worms are still there on the Internet but are tapering by the help of built-in security provided by Operating Systems, IPS, IDS and Firewalls. However, DoS attacks which are widely known from 90's continue to remain as a big threat for Internet.

From, the survey of Arbor Networks [5], 12,000 DoS attacks occur per week, states the severity of the problem.

IPS, IDS and Firewalls are used to protect end systems and servers. All these end systems are having different types of security features to protect themselves from attacks over Internet. However, from the recent news [1-4], some of the high profile servers were brought down by DoS attacks. DoS attacks afford the targeted servers or end systems in-spite of security provided in their security systems.

This motivated us to investigate some of the built-in security features provided on the Server operating systems, Firewalls and IPS in defending against the DoS attacks. The Microsoft Windows Server is mostly used worldwide compared to the other Server operating Systems because of the security, reliability and efficiency provided by them [6]. We chose the Microsoft Windows 2003 Server and recently released Microsoft Windows 2008 Server and planned to observe their ability in defending against the DoS attacks. We also planned to test the performance of Juniper Networks – Netscreen 5GT Firewall/IPS, in defending against the DoS attacks and the availability provided by it at the time of providing security for legitimate users. Also in this thesis, Cisco ASA-5510 IPS is planned to be tested under DoS attacks. Cisco Router/IPS is having special features in defending against DoS attacks. Security and availability provided by this IPS is evaluated at different loads of attack traffic.

### 1.1 Denial of Service Attacks

Denial of Service (DoS) attack is a challenging problem for the Internet. This is increasing over Internet and causing a lot of damage financially by using the loopholes of the Internet protocol [7, 8]. The attack which causes the legitimate users not to perform their own tasks by consuming all computing resources of victim computer is called a Denial of Service attack. DoS attacks can target a simple individual end system, or a major Internet commerce of Government, or Private organizations, or even the root infrastructure of the Internet, no one is exempt from these attacks. An attacker may target the victim, for personal reasons, or for political reasons and sometimes for even financial gain.

Master card, Visa Websites were brought down by Wikileak supports using DDoS attacks[9].Recently during memorial day-2009 there were a series of DoS attacks on the servers of US and South Korean governments [1] and then on august 6$^{th}$ 2009, servers like Twitter, Facebook, Livejournal, Google's Blogger and Youtube were under DoS attack. Where Twitter was down for several hours [2]. Compromising thousands of systems over the Internet, involving them to flood some millions of packets towards the targeted victims, strengthening the attack traffic. More than 12,000 DoS attacks per week [5], results in a loss of millions of dollars explains the states the severity of these attacks.

Denial of Service attack can be launched by sending large quantity of illegitimate attack packets towards the victim. Where all these packets consume critical resources at the victim, either the network bandwidth, or processor resource or even memory resources. This results in no service for the legitimate users [10, 11]. Victim systems may crash in handing the attack traffic or spend majority of its time processing attack traffic, which keeps it from surving the

legitimate users. DoS attacks may take the vulnerabilities of a targeted system as advantage or even flood large quantity of illegitimate traffic to bring down the targeted victim.

DoS attacks can be launched by taking advantage of the vulnerabilities in the end system. Attackers will first try to scan the victim's network and find the vulnerabilities of that network [12, 13]. Every individual user or corporate servers will have operating systems on their machine, which provides different types of protection from various attacks. On the other hand, these protection features can also lead to Denial of Service due to consumption of resources in the way of defending against the attack. If a malicious message represents an unexpected input which causes the target system or an application go into infinite loop. This situation causes the machine to freeze or reboot. This leads to denial of service on the victim. From paper [14], the McAfee Security Centre 2009 and 2010 have a vulnerability, which causes DoS by consuming the main memory when defending against the external Ping flood packets.

On the other hand, by flooding the packets on the victim system or victim network, the attacker consumes all the resources of the network or the victim computer. This can also prevent legitimate users from accessing Internet service. From paper [15], Microsoft's Windows Vista and Apple's leopard operating systems were not capable of protecting them self's against the Internet Control Message Protocol (ICMP) – Land Attack. Where Windows Vista crashed at 30 Mbps load of land attack traffic due to depletion of available main memory. In the case of Apple's leopard operating system, the processor exhaustion reached a dangerously high CPU utilization of approximately 86% 1Gbps of ICMP – Land attack traffic. Land attack is flood type of DoS attack, where ICMP packets are flooded towards the victim.

### 1.1.1 Distributed Denial of services (DDoS) Attacks

Distributed Denial of Service (DDoS) Attacks compromises a large number of unprotected machines on Internet and uses them to flood attack traffic towards the targeted system. Denial of Service attacks which requires the flood of traffic or even traffic, which cannot be traced, then this technique is used [16-20]. The attack traffic is amplified in magnitude by using the compromised or unprotected machines over the Internet [21]. DoS attacks are also possible without distributed techniques. However, flooding type of attacks, where attacker targets a large server would be difficult for overwhelming the server's resources with his own resources. It also weakens the potential effect of tracing back the attacker by using this distributes technique, which can be possibly by using spoofing technique [22-26].

### 1.1.2 Spoofing

In the Internet, identity for an individual is the IP address. IP Spoofing forms a platform for a larger number of Denial of Service attacks. Fake IP addresses are used as the source address of the IP packets used in the attacks [27-30]. When a malicious program is installed on an unprotected system over Internet they will act as Zombies. These Zombies can create packets by setting fake or spoofed source IP addresses and target them towards the victim as directed by the legitimate users from Internet. The attack traffic can come from different places on the network whole over the world or even originate from the local network with spoofed IP addresses. Due to IP spoofing technique, distinguishing between attack packets and legitimate traffic is difficult because, it seems like the packets are coming from different sources and it will be difficult to identify the attacker [31].

### 1.2 Classification of DoS attacks

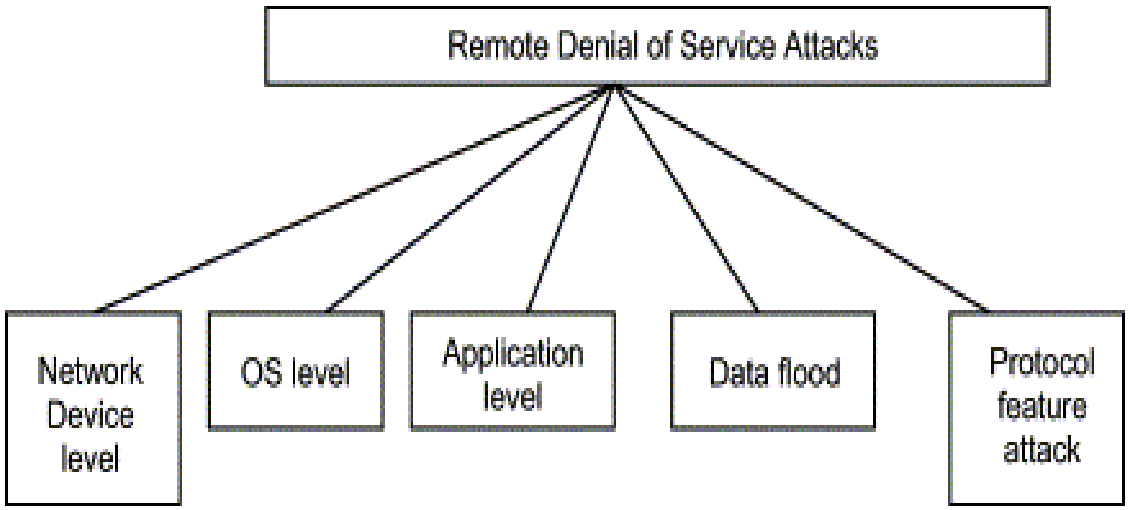



**Figure 1.1:** Classification of DoS Attacks [23]

DoS attacks are widely known from 90's and first large scale appearance of DoS attack is in mid-99's, but still attackers follow the same attack techniques. DoS attacks can be classified based on the protocol as illustrated in figure 1.1 [23].

In this protocol level classification, there are network devices level, OS level, Application level, Data flood level and Protocol feature level classifications of DoS attacks. Where network device level attacks caused by taking advantage of vulnerabilities in the software's or by consuming the hardware resources. Operating systems (OS) level attacks based on the loopholes find in implementation of the protocols which are different for different Operating Systems. Application level attacks exploits vulnerabilities of applications on the systems or by just flooding large amounts of illegitimate traffic to consume the critical resources on the system by using the applications on them [10]. Data flood type attacks concentrate on the network bandwidth just by overwhelming meaningless illegitimate traffic to consume all the available

bandwidth and cause denial of service for legitimate users in that network. Protocol based attacks take advantage of the features of standard protocols and in Denial of Service Attack

The following section includes different Denial of Service attacks, which are used in this thesis work because of their popularity with hackers, and these attacks are known to have caused significant denial of service on Internet [10].

### 1.2.1 Transmission Control Protocol – SYN Attack

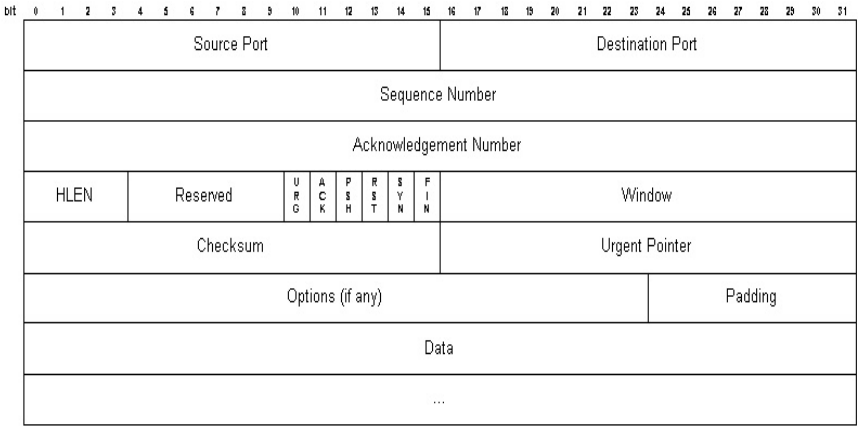



**Figure 1.2:** Transmission Control Protocol [33]

**1.2.1.1 Transmission Control Protocol.** The Transmission Control Protocol (TCP) is a connection-oriented protocol [33]. 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 (Figure 1.2). TCP layer provides reliability, flow control, and congestion control, when the connection is formed between two hosts. 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 1.3).

**1.2.1.2 Three – Way Handshake.** 3–Way Handshake is the connection mechanism used in the Transport Control Protocol. From figure 1.3, we can see the connection established between the HTTP client and HTTP server [33]. 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.

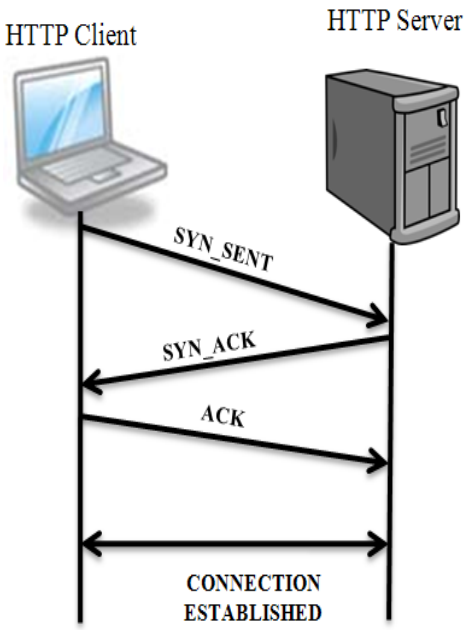



**Figure 1.3:** Three – Way Handshake

**1.2.1.3 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 1.4), or if one of the hosts closes the connection without acknowledging the other [34-36]. 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.

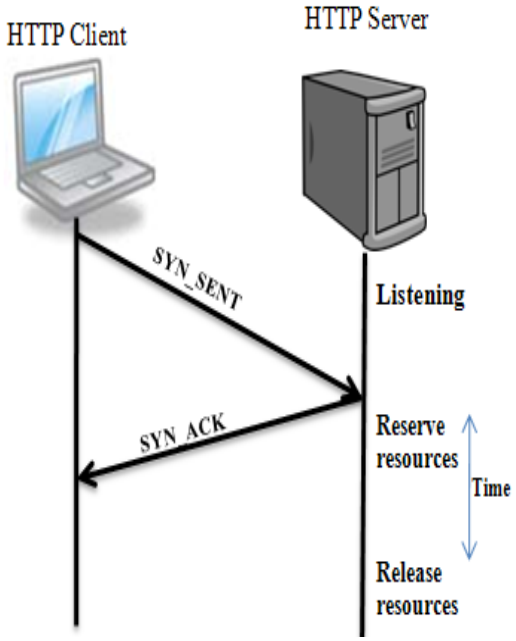



**Figure 1.4:** TCP Half Open Connections

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

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

**1.2.1.4 TCP SYN Flood Attack.** From figure 1.5, 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. While sending the reply, server reserves some resources for the client and waits for final ACK to arrive from the client [37-39]. If the source IP address was a spoofed one, then the server waits up to timeout time and releases the resources if final ACK didn't arrive.

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

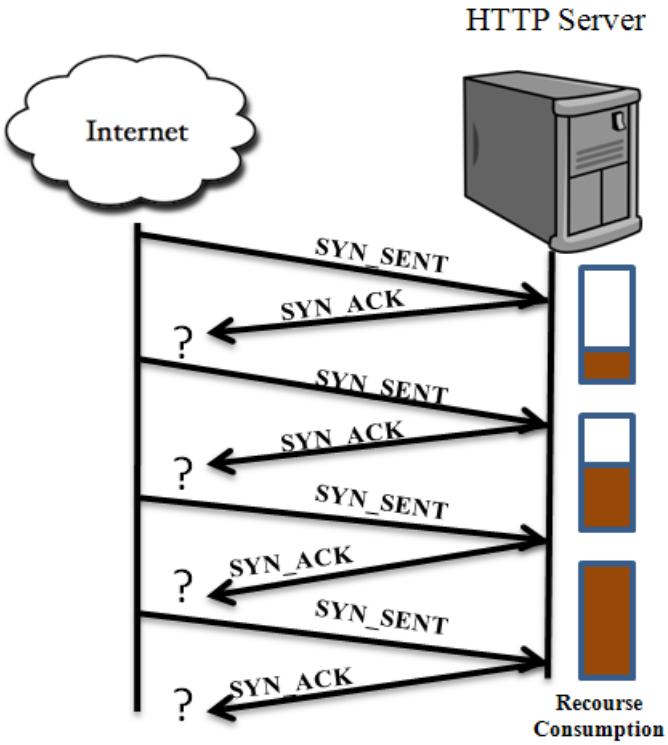



**Figure 1.5:** TCP-SYN Flood

### 1.2.2 Internet Control Message Protocol – Ping Attack and land Attack

**1.2.2.1 Internet Control Message Protocol based Denial of Service attacks.** In this DoS attack, attacker takes advantage of ICMP protocol in launching an attack. Internet Control message Protocol (ICMP) is used to diagnose and report any error in a network. This is defined in Internet Protocol (IP) suit (RFC 792) [40]. For example, "Destination Unreachable" is an ICMP message which is generated towards source, when the packet is not able to reach the destination. Ping is an ICMP message used for checking host availability in a network.

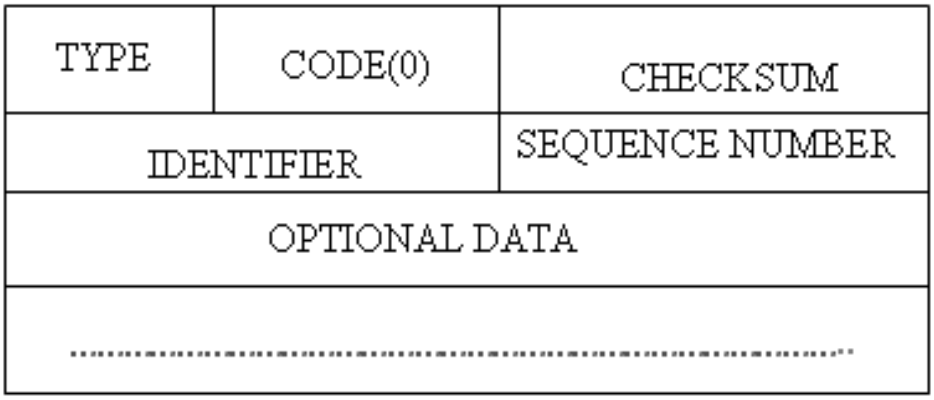



**Figure 1.6:** ICMP header format [40]

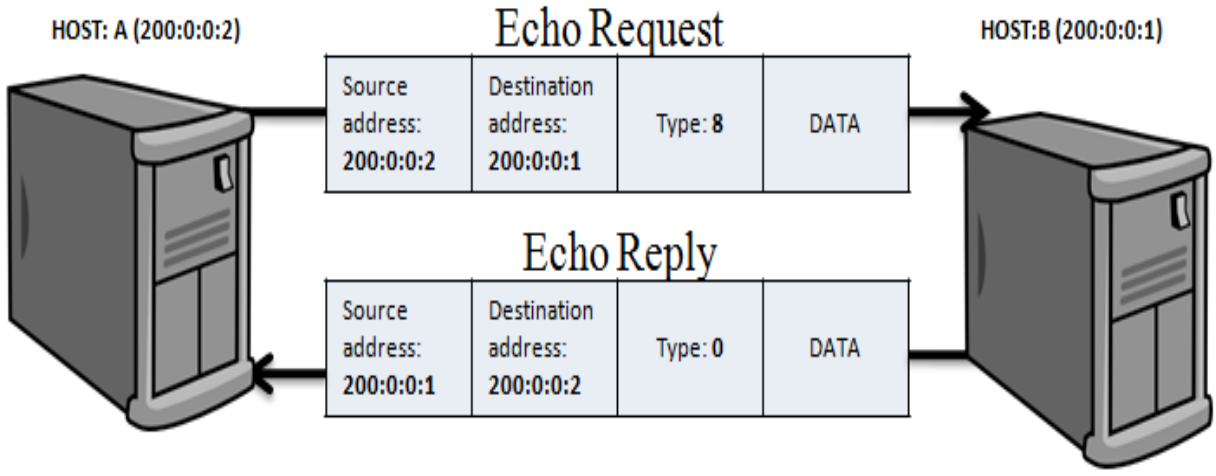



**Figure 1.7:** Ping utility

**1.2.2.2 Ping Utility.** 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 [40].

Figure 1.7 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 1.6) in Echo Request is 8, and in Echo Reply is 0.

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

**1.2.2.3 ICMP Ping DoS Attack.** ICMP Ping DoS attack initiates 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 sent towards the victim host. When the host receives the echo requests, it should reply with the same data to the source host with Echo reply message. The attacker’s intention is to consume the resources of the victim host. ICMP echo requests when flooded towards the victim host, it can consume resources on the victim computer in performing the job of sending echo replies for all the echo requests [41, 42].

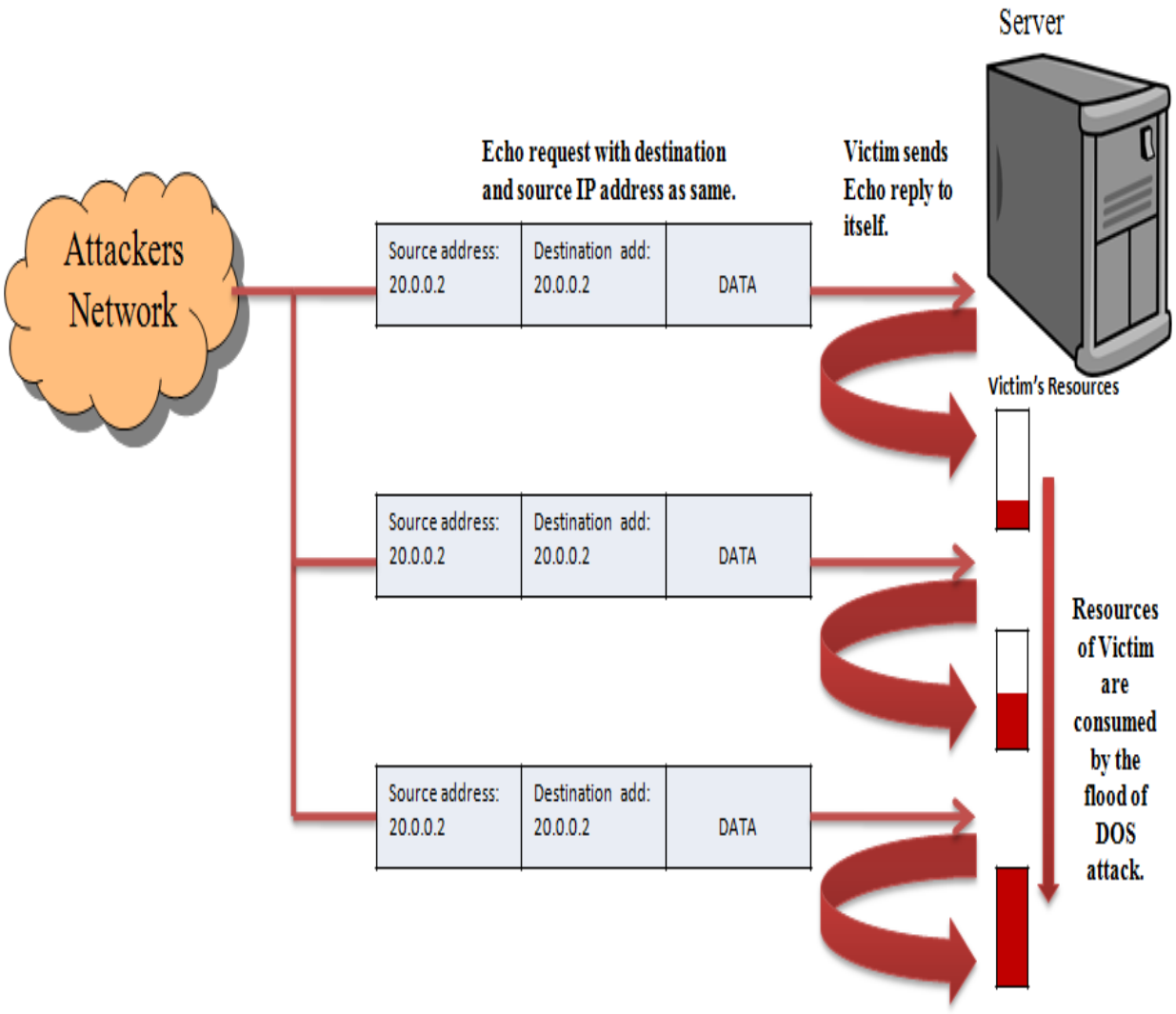



**Figure 1.8:** ICMP Land Attack

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 prevent the victim from serving the legitimate users.

Victim, who comes across this type of attack in a network, thinks that there was some problem in the network. However, it is difficult to identify the attack, because attack traffic can be with spoofed IP addresses [43, 44].

**1.2.2.4 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, this can result in a DoS attack called ICMP Land Attack [45, 46].

When the victim is flooded with continuous ICMP Echo Request having identical source and destination IP address, it needs to reply for all Echo requests. This may utilize a lot of resources. As, the echo requests are having source and destination IP addresses identical, all the Echo replies sent by the victim are received by the victim and eventually dropped. This may utilize more resources then the time when victim receives only echo requests (Figure 1.8).

### 1.2.3 User Datagram Protocol Flood Attack

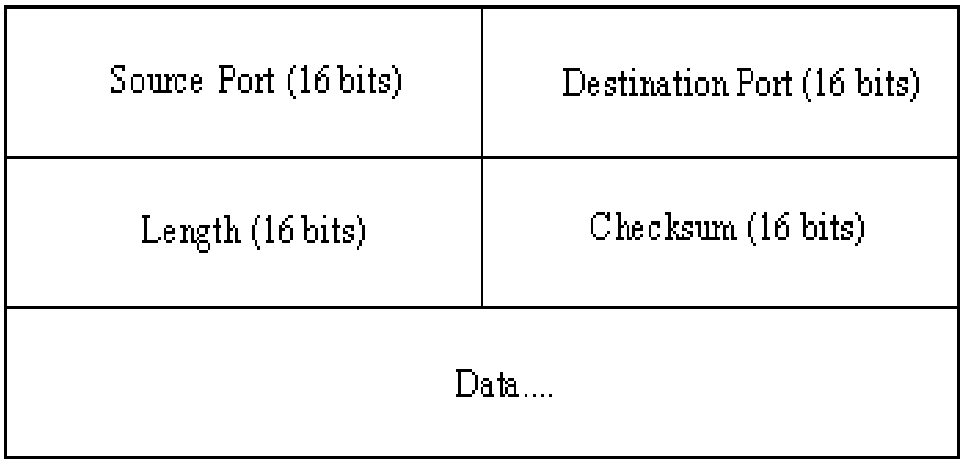



**Figure 1.9:** UDP Header format

**1.2.3.1 UDP Flood Attack.** UDP Flood attack is Layer-4 type DoS attack. UDP Flood vulnerabilities have been discovered during the year 1998-2000. In this attack a barrage of UDP packets are sent to the victim computer either on selected UDP port or on random port (Figure

1.9). The targeted system processes the incoming datagram to determine which application it has requested on that system by referring the port number. In case if the requested application is not present on the system or the requested port is not open on the target system, an ICMP Destination Unreachable message is sent to the source address. The 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 reply back with ICMP Destination Unreachable messages in case if the application was not present on the system, which consumes all the resources of victim [47-49].

## 1.3 Thesis Outline

The main goal of this Thesis is to test and evaluate the performance of Internet equipment under common Denial of Service attacks. Internet is combination of servers, which are used to store and share the information; security systems, which plays important role in protecting the private network from the threats over the Internet, like firewall and Intrusion Prevention System (IPS) ; routers for routing the WAN traffic; switches for switching the LAN traffic, and End systems. Security is provided at the Network level like Firewall/IPS and also at Host level like Host based firewalls. This thesis was narrowed towards the protection capabilities of most critical and important components of the Internet which are helpful in maintaining secure communication.

In evaluating servers, we selected the server operating systems of Microsoft, Windows server 2003 and Windows server 2008, which are used by large number of people throughout the world. Regarding security systems, Juniper Networks Netscreen 5GT firewall/IPS and Cisco

ASA 5510 Router/IPS, which are with Denial of Service security features on them are selected for our experiments.

This thesis is organized as follows: Chapter I is an introduction to DDoS attacks and background for our experiments. Chapter II presents the inbuilt capability of Microsoft Windows Server 2003 SP-2 and Microsoft Windows Server 2007 SP-1 in defending against the DoS attacks. This chapter tells us how these Server Operating Systems are affected by DoS attacks, and also shows their influence on the legitimate client connections in real time environment. Chapter III shares the inbuilt capabilities of Juniper Networks Netscreen 5GT firewall/IPS in defending the DoS attacks. This chapter provides the results of the firewall/IPS, which needs to protect the local network from the threats over the Internet, when stressed by DoS attacks. Chapter IV explains the protection techniques of Cisco ASA 5510 Router/IPS against the DoS attacks. This chapter also includes the results, when this Cisco ASA is stressed under different DoS attacks. These results expose the availability provided by the Cisco ASA, along with providing security from illegitimate traffic at different loads of DoS attack. In Chapter V, we conclude this thesis and suggest some possible future work. This thesis can be expanded in testing the influence of DoS attacks over Internet on other operating systems, newly developed Security systems and also on the IPv6 protocol loop holes. Finding the effectiveness of those systems and protocols against DoS attacks can be helpful in transferring Internet as safe medium for communication, to our next generations.

# CHAPTER II

## EVALUATION OF SECURITY PROVIDED BY WINDOWS SERVER 2003 AND WINDOWS SERVER 2008 UNDER COMMON DENIAL OF SERVICE ATTACKS

People depending on the Internet for their daily activities are increasing rapidly. Internet is used for sharing and storing valuable information electronically with the help of servers. What happens if a server was brought down by some Internet attack such as DDoS attack? It may cause financial damage or even terrible effects to human safety, if that server relates to some critical services, which are using the Internet for their transactions. Almost every server on the Internet are provided with Firewalls, Intrusion Preventio0n system ( IPS) or intrusion Detection System (IDS) having different types of security features to protect themselves and their private networks from security attacks on the Internet. Despite protections, DoS attacks can reach the targeted servers and prevent legitimate users to connect to the server [50-52].

This motivated us to investigate the inbuilt security features provided on the Server Operating Systems in defending the DoS attacks when the attack traffic reaches servers, crossing all other security systems. Microsoft Windows is used worldwide due to its security features, reliability and efficiency [53, 54], which are of interest in this chapter. In this chapter we evaluate Microsoft Windows 2003 Service Pack-2 Server and newly released Microsoft Windows 2008 Service Pack-1 Server for their ability in defending against common DoS attacks.

## 2.1 Experimental setup

In the Networking Research Lab (NRL) at The University of Texas-Pan American, we launched different types of common DoS attacks to observe the inbuilt ability of servers 2003 and 2008 in defending against the attack, servers are configured as HTTP [55] Server (Web Server). Same computing hardware platform was used in the experiments that deployed different servers 2003 and 2008 as given below:

1. Microsoft Windows Server 2003 Service Pack-2 (Enterprise x64 Bit Editions) – on Intel ® Xeon® CPU E5345 @ 2.33 GHz, 2.33 GHz [56] with Memory (RAM): 8.00GB.
2. Microsoft Windows Server 2008 Service Pack-1 (Enterprise x64 Bit Editions) - on Intel ® Xeon ® CPU E5345 @ 2.33 GHz, 2.33 GHz with Memory (RAM): 8.00GB.

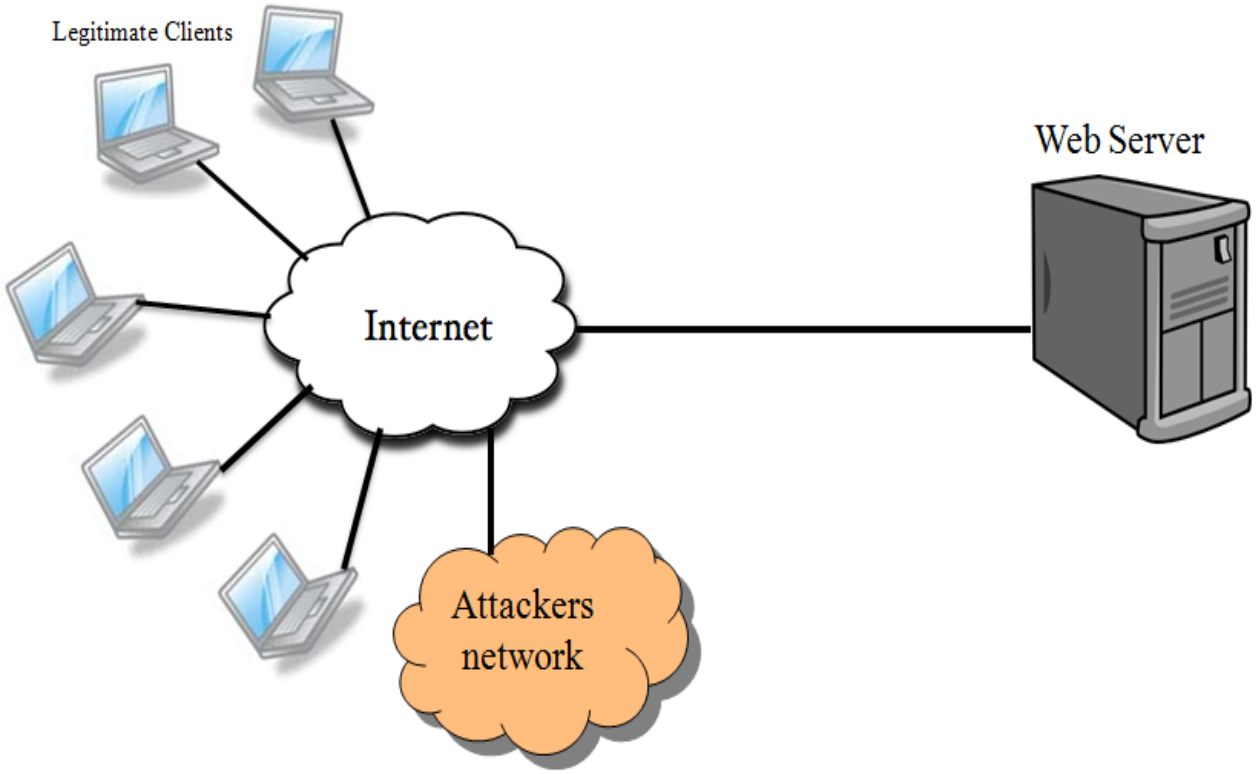



**Figure 2.1:** Experimental Setup

## 2.2 Default inbuilt Security

TCP occupies 80% of the total traffic on the Internet, and so it commonly used by attackers [57]. Because of these reasons, all manufactures concentrate in securing the TCP featured applications along with the other protections. Windows Server OS also provided built-in security feature called “SynAttackProtect”, which is enabled by default for Windows Server with service packs installed. This protection reduces the amount of retransmissions of the SYN-ACKS, which also reduces the allocated memory for TCB entry resources for the incoming SYN segment until the full connection is established by completing three-way handshake process. This protection mechanism is activated when the TcpMaxHalfOpen and TcpMaxHalfOpenRetried threshold levels are exceeded [58, 59].

TcpMaxHalfOpen is a parameter which is used as a threshold for the number of connections in the SYN-Received (SYN-RCVD) state before the SynAttackProtect protection begins to function. By default, this threshold is set to 500 Connections in the Windows Server Enterprise Edition with service pack. And TcpMaxHalfOpenRetried is the parameter which is used as a threshold for the number of connections in SYN-RCVD state for which one retransmission of SYN-ACK segment has to be sent before the SynAttackProtect begins to function [60, 61].

We compare performance of security features and protection provided by Microsoft for Windows 2003 and 2008. It is easy for an attacker to target the system and compromise it if he knows there is an open port with no security. On Windows Servers we have a protection with the Firewall to protect all the unused ports or to block the packets that are targeted to the unused

ports. This can be protected from attack traffic, which may consume all the resources on the server [62].

## 2.3 Evaluation of Security Provided by Microsoft Windows Server 2003 under common DOS attacks

### 2.3.1 Evaluation of Security Provided by Microsoft Windows Server 2003 under TCP-SYN attack

In this case, the legitimate HTTP traffic from different clients having individual IP addresses are initiated from Internet towards the targeted Web Server, which is configured on the Microsoft Windows Server 2003 (SP-2). This resulted in a maximum of 20,000 connections per second. TCP-SYN attack traffic consists of SYN packets that are flooded towards the server at different loads. At, each attack load the corresponding processor consumption, memory consumption, number of attack packets received and packets sent by the server are recorded to understand the behavior of the server 2003 under TCP-SYN attack.

When the TCP-SYN attack was sent to the server the SYN packets that are sent towards the server will not only consume resources for processing those packets but also reserve some resources on the server to maintain connection between the server and client, which is helpful in building up a reliable data transfer.

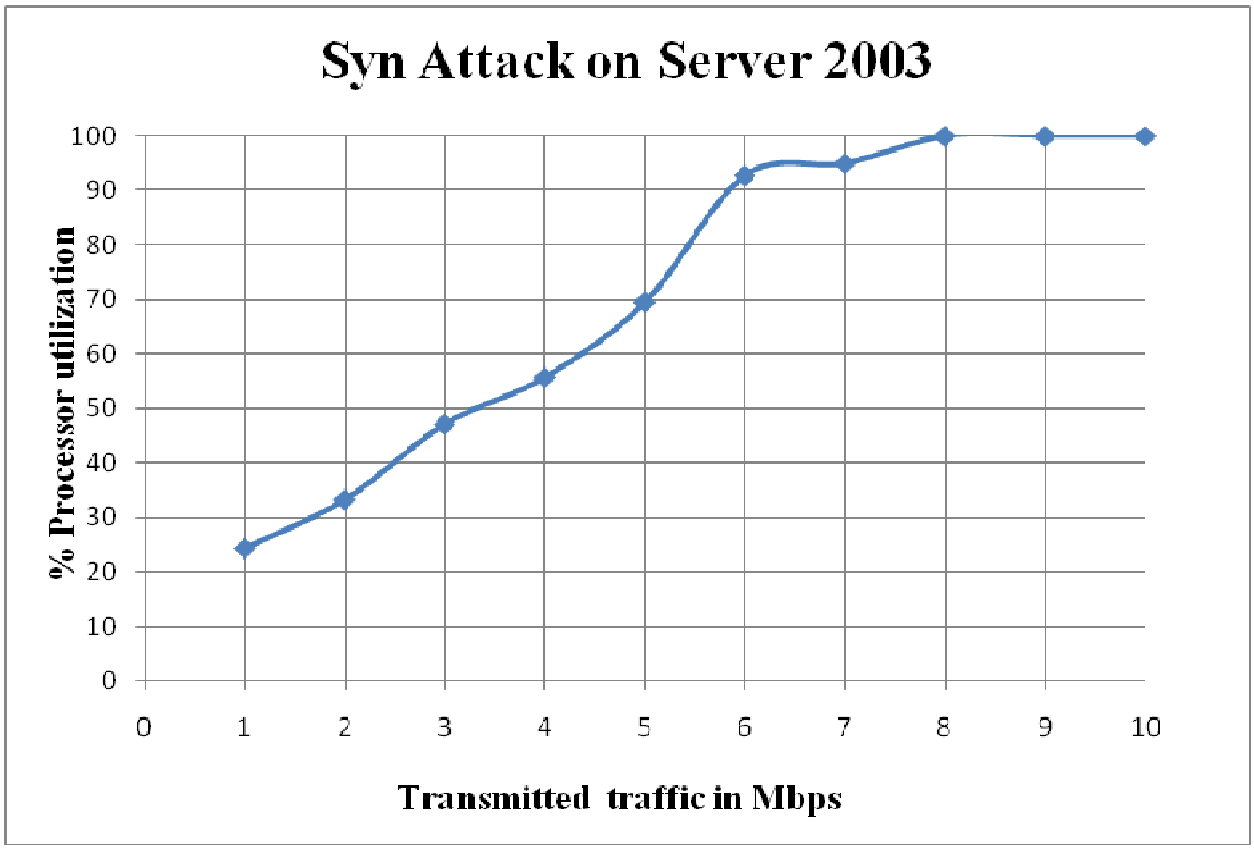



**Figure 2.2:** Processor utilization Vs TCP-SYN Attack Load on Microsoft Windows Server 2003

TCP-SYN attack at different loads varying in the range from 0Mbps to 10Mbps, are sent towards the server. The influence of the attack traffic on the resources of the server, with the default configuration set by the Microsoft, explains the effect of TCP-SYN attack on the server. The processor resources of the server reaches to 100% at 8Mbps, which is a small amount of traffic compared to its link rate of 1 GB (Fig. 2.2 and Fig. 2.3).

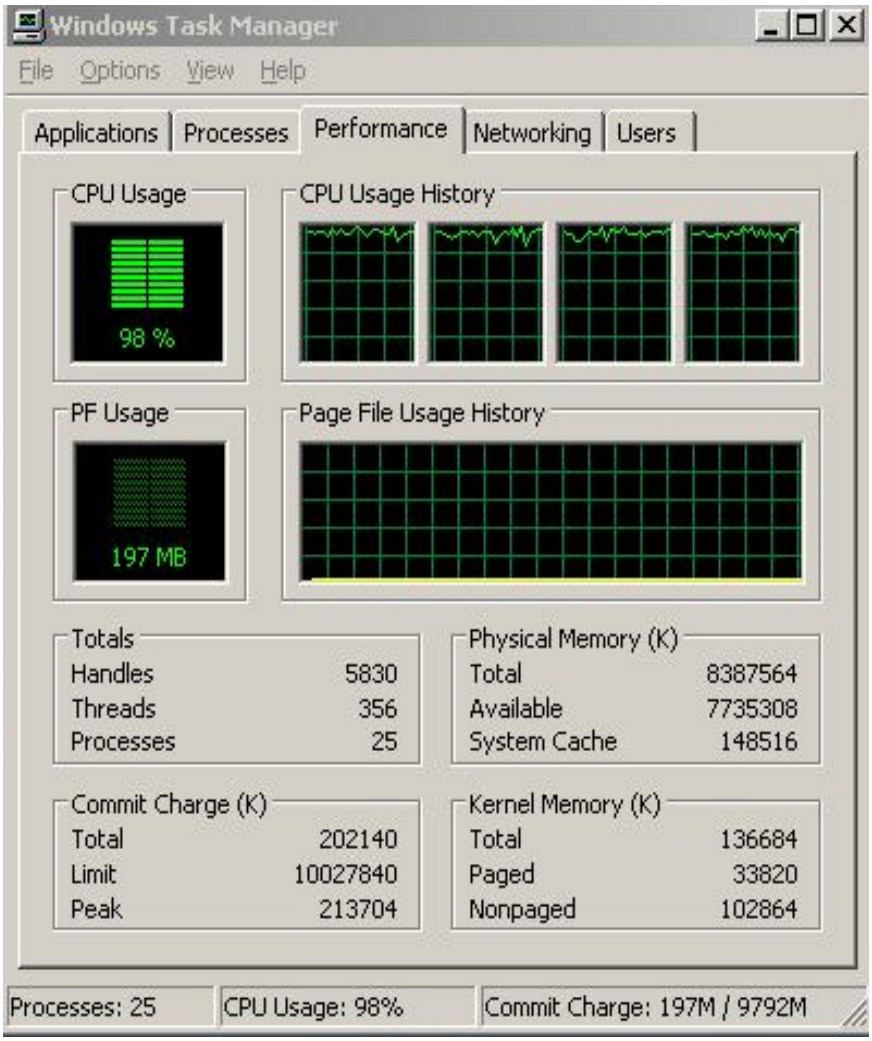



**Figure 2.3:** Snapshot of the processor consumption at 6Mps Attack Load on Server 2003

In the real time, if this server which is serving thousands of clients on Internet is attacked by SYN attack, then what will be the security and availability provided by server.

For the experiment, 20,000 client HTTP connections were maintained to sending TCP attack. TCP-SYN attack with traffic loads in the range of 0 to 10 Mbps. This experiment states the security and availability provided by the Windows Server 2003 at real time.

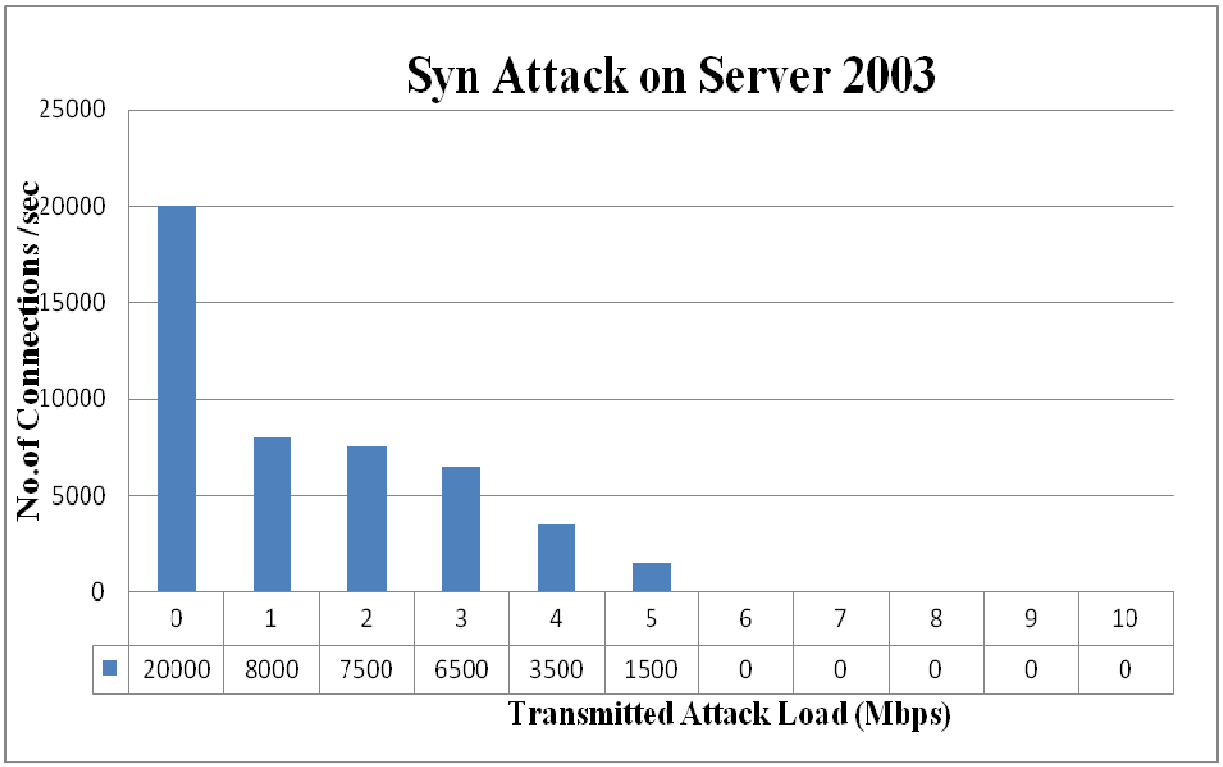



**Figure 2.4:** Number of client connections per second Vs SYN Attack load for Windows Server 2003

From Fig 2.4, without attack load, the total number of connections are 20,000 and it reached zero at 6Mbps of attack load. No legitimate users are able to get service from server after the attack traffic reaches 6 Mbps, which left no limited resources for legitimate users.

### 2.3.2 Evaluation of Security Provided by Microsoft Windows Server 2003 under UDP-Flood attack

In this case a flood of UDP packets are sent to random ports of server, requesting for a service at that port. When the server receives the UDP packet with a port number where no application is available then, the server sends an ICMP Destination Unreachable Message back to the source address. And if the server is flooded with a barrage of such requests, of the system resources can be consumed resulting in denial of service for legitimate users.

For this experiment, UDP Flood attack traffic at varying loads is sent towards server deploying Windows Server 2003 Operating System on it, values of the processor utilization, memory utilization, packets received and packets sent were observed and compared under two cases; first is without allowing all the incoming connections, and second is with protection on firewall.

It is observed that Windows 2003 server consumed a maximum of 83% of processor resources (Fig. 2.5). The memory resources are not influenced by the UDP Flood attack. The memory consumption stays constant at 470Mb in the case of no protection on the firewall (Fig 2.5). On the other hand, processor was consumed to the maximum of 35%, with memory at 470MB throughout the experiment in the case of protection enabled on the firewall (Fig. 2.5 and Fig. 2.6).

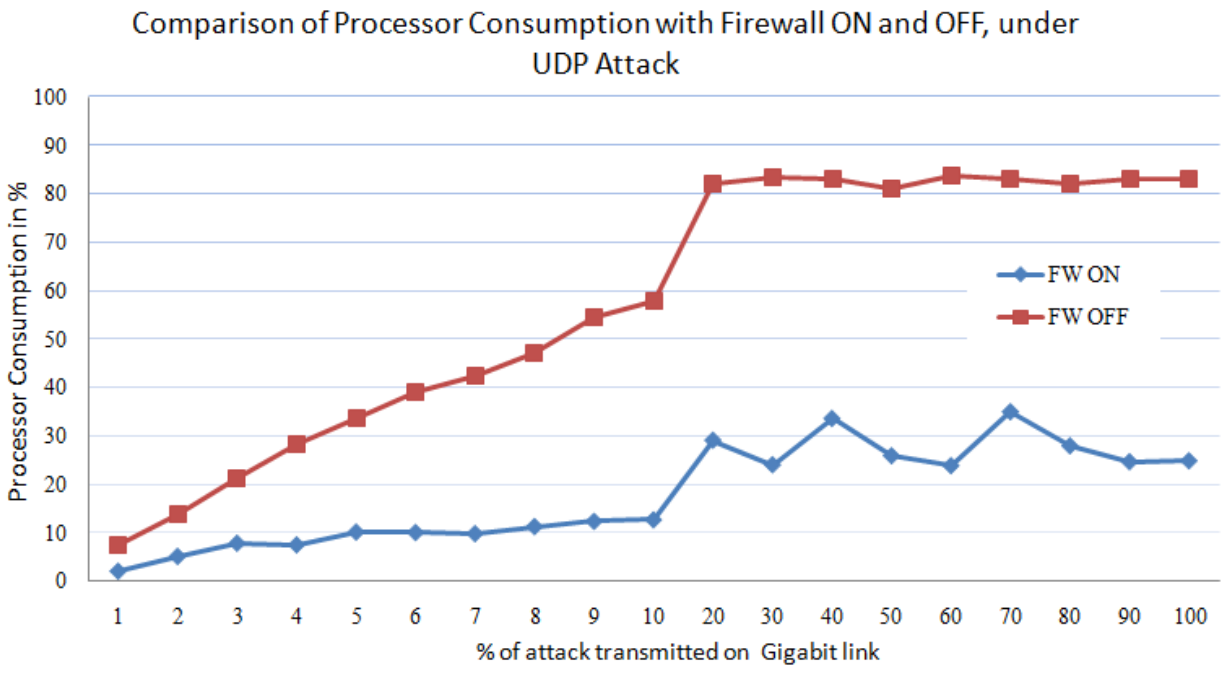



**Figure 2.5:** Comparison of processor consumption by UDP-Flood Attack on Windows Server 2003 with Firewall OFF and Firewall ON

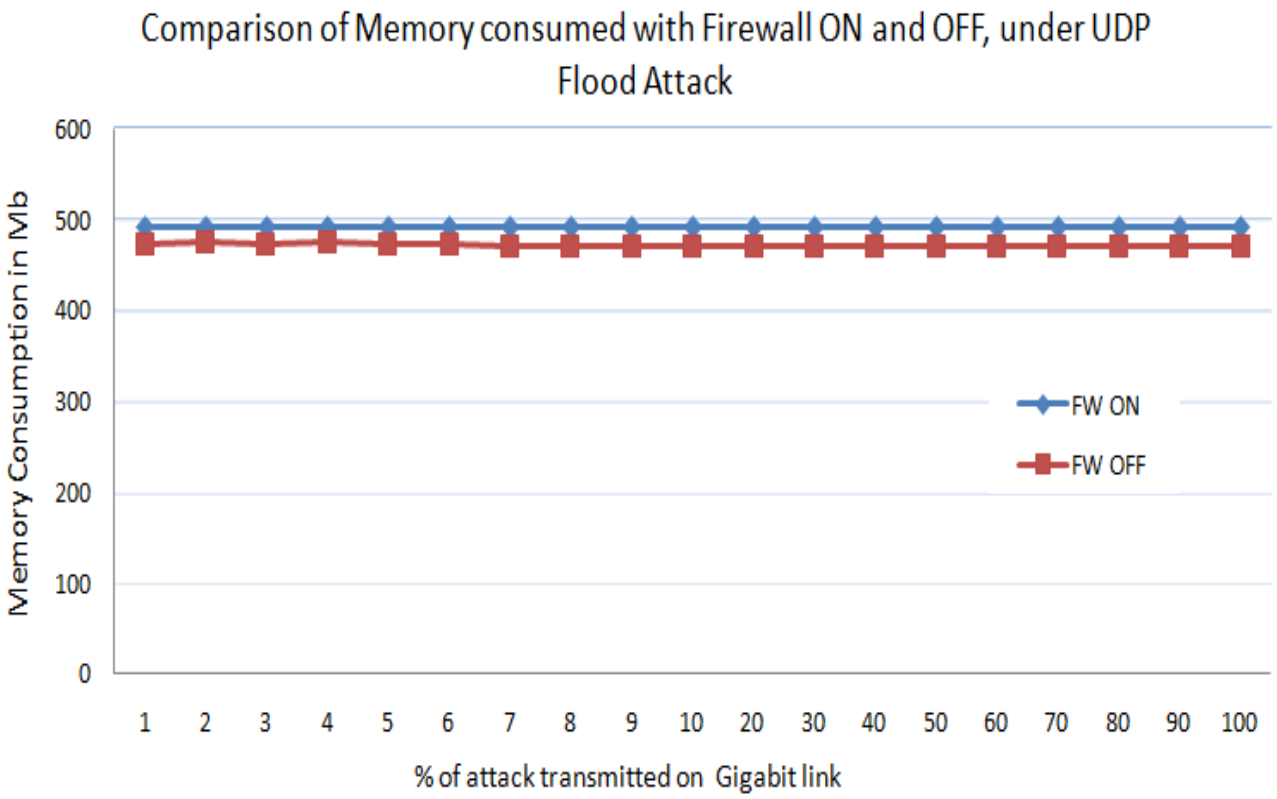



**Figure 2.6:** Comparison of memory consumption by UDP-Flood Attack on Windows Server 2003 with Firewall OFF and Firewall ON

The reason behind the maximum consumption of 83% processor resources, after reaching 20% (200Mbps) of attack load is, due to the maximum of 500,000 UDP datagram's received by the Server at 20% (200Mbps) of attack load, and the maximum of 250,000 ICMP Destination Unreachable Packets sent by the server due to no existing application on the port that is requested by attacker (Fig's 2.7 and 2.8). This is because of allowing all the incoming connections by the firewall and replying to all the datagrams received by the server, lot of processor resources and bandwidth were consumed. Consumption of processor and bandwidth to the dangerously peak levels can lead to the Denial of Service attack, which may results in no services to the legitimate users.

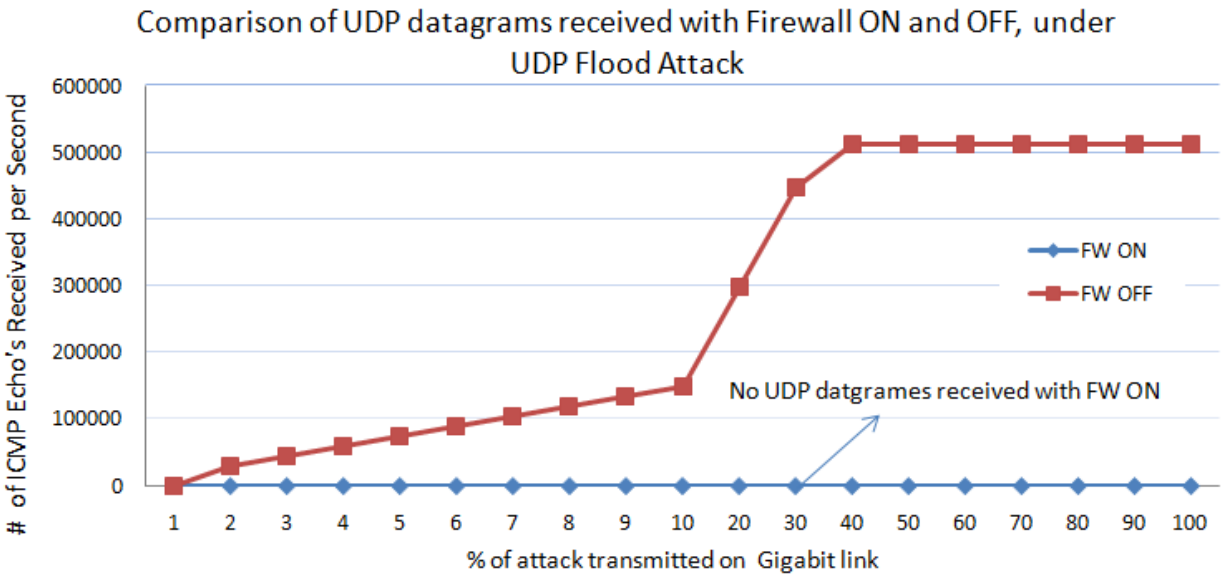



**Figure 2.7:** UDP datagram's received at the time of UDP-Flood Attack on Windows Server 2003 compared when Firewall was OFF and when the FW was ON

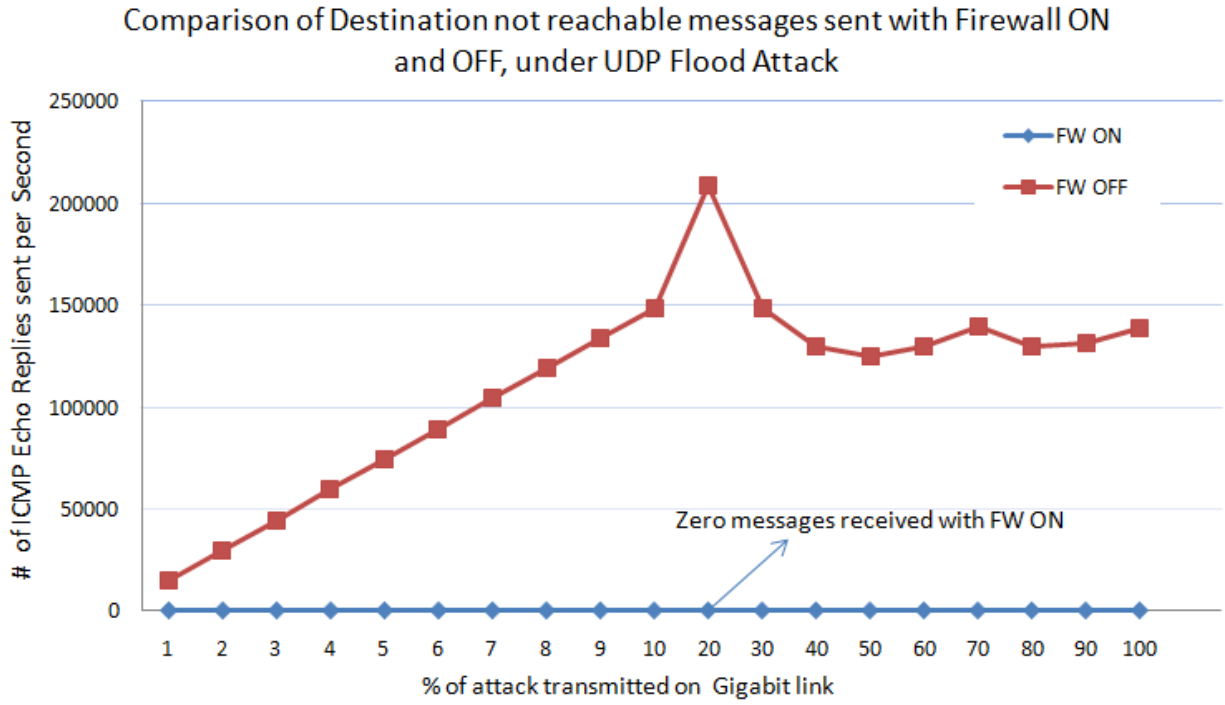



**Figure 2.8:** ICMP-Destination Unreachable packets sent at the time of UDP-Flood Attack on Windows Server 2003 with Firewall OFF compared with Firewall ON

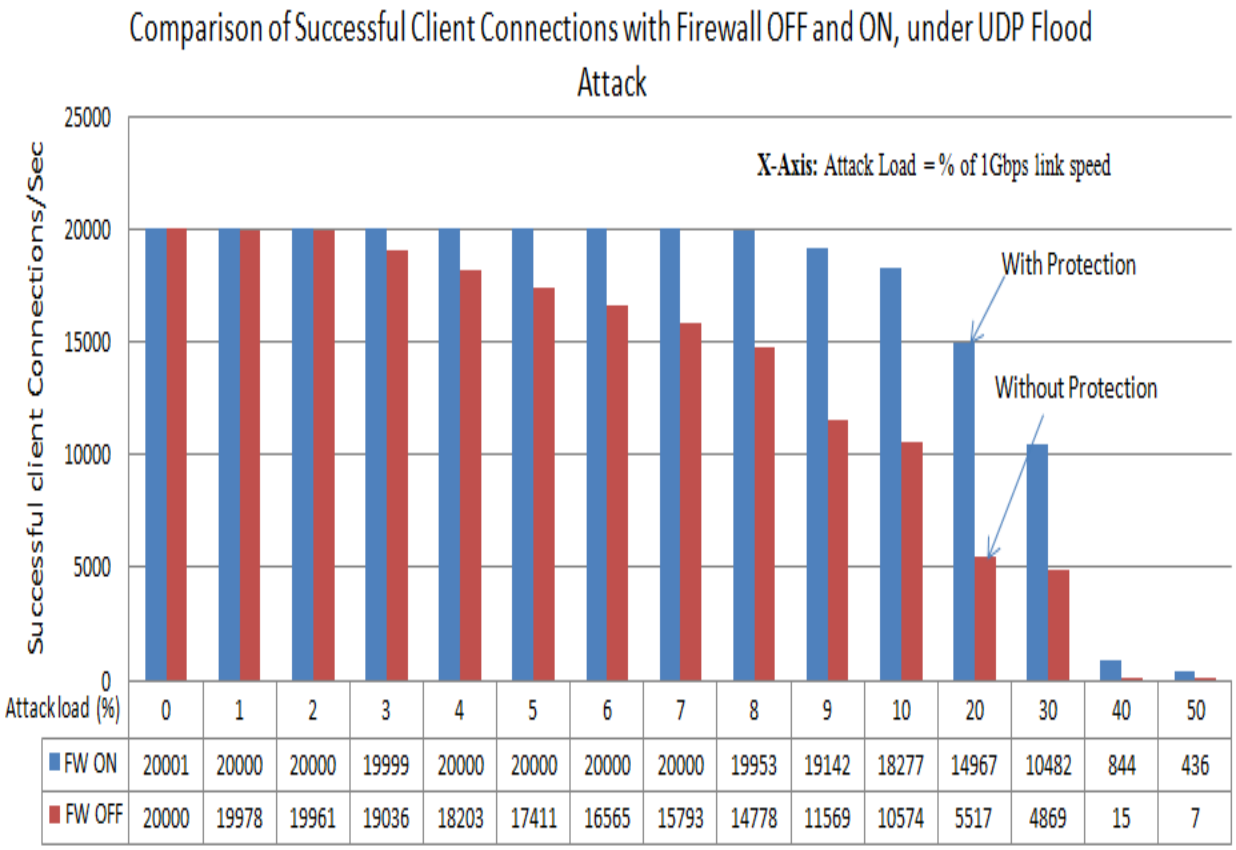
The reason behind the maximum processor utilization of just 35% when firewall is ON is due to the protection offered by the firewall by dropping all the UDP packets. Though the operating system is not processing all the incoming UDP packets, considerable resource exhaustion can be observed that may result in DoS attack to legitimate users (Fig's 2.7 and 2.8).

In the real-time environment (Internet), when the legitimate users are receiving services from the server is at the same time if the UDP-Flood attack is launched on the server, then the influence of this attack on the legitimate users, can be observed from following experiments. Where HTTP legitimate traffic with 20,000 Client connections/Sec is maintained towards the server, which is simulated as the traffic coming from different users (different IP address) from Internet, and the attack traffic of different loads in a range of 10Mbps to 1Gbps is directed towards the server. The comparison of successful TCP client connections formed between the server and the legitimate users at the time of attack at varying loads is observed under two cases: firewall protection enabled and firewall protection disabled are given in Fig. 2.9.

From Fig. 2.9, it is observed that the successful client connections are formed with the server are 20,000 per second with no attack traffic. However this number decreases with the increase of the UDP-Flood attack load and results in almost zero client connections at 40% (400Mbps) of the attack load with no protection enabled on the firewall. When the server is protected with the protection on the firewall blocking all the unused ports, it leads to some improvement in the number of client connections compared to the case with no protection.

However the successful connections are brought down to less than 500 connections at 500Mbps of attack load. The total number of connections are 10,574 in case with no protection and with protection they are 18,277 at 10% (100Mbps) attack load. At 30% (300Mbps) attack load successful connections are brought down to 4,869 with no protection, which is lower when

compared to the case with protection enabled, which is recorded as 10,482 connections per second.




| Attack load (%) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 20 | 30 | 40 | 50 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FW ON | 20001 | 20000 | 20000 | 19999 | 20000 | 20000 | 20000 | 20000 | 19953 | 19142 | 18277 | 14967 | 10482 | 844 | 436 |
| FW OFF | 20000 | 19978 | 19961 | 19036 | 18203 | 17411 | 16565 | 15793 | 14778 | 11569 | 10574 | 5517 | 4869 | 15 | 7 |

**Figure 2.9:** Successful client connections/Second formed at the time of UDP-Flood Attack on Windows Server 2003 with Firewall OFF compared with Firewall ON

For lower UDP attack loads, we observe that Windows server 2003 is defending better with protection enabled on the firewall, when compare with the protection disabled, on the FW. But at higher loads of attack traffic, even with the protection enabled on the Firewall Windows server 2003, it is not able to withstand the UDP attack flood and is not able to serve the legitimate users resulting in almost less than 500 successful client connections at 50% (500Mbps) UDP attack load.

### 2.3.3 Security Provided by Microsoft Windows Server 2003 under ICMP PING-Flood attack

In this case ICMP Echo requests are flooded towards the server, where server replies with Echo reply packets, which states that the server is available in the network. This process consumes some of the resources of the server. If these Echo requests are flooded, all the critical system resources such as processor, memory and bandwidth will be consumed resulting in denial of service for the end users. And this ICMP attack traffic of layer - 3 is sent to server, making it process and reply to all echo requests. This consumes the critical resources on server, which leads to DoS attack. That results in no limited resources for the legitimate users for their services.

In this case ICMP Ping Flood attack traffic at varying loads from 10Mbps to 1Gbps is sent towards server deploying Windows Server 2003 Operating System on it, and the processor utilization, memory utilization and packets received and packets sent are measured. These results are compared under two configurations: first is without protection from built in Firewall, allowing all the incoming connections. Second configuration is with protection from firewall, where unused or unsafe connections are blocked in reaching the server that can cause damage to the server. It is observed (Fig 2.10) that Windows 2003 is consumed a maximum of 73% of processor resources and the memory was not influenced by the attack load, which is occupied near 460Mb in the case of no protection from firewall. The processor is consumed a maximum of 50%, with memory occupied at 460Mb in the case of protection enabled on the firewall (Fig. 2.10 and 2.11).

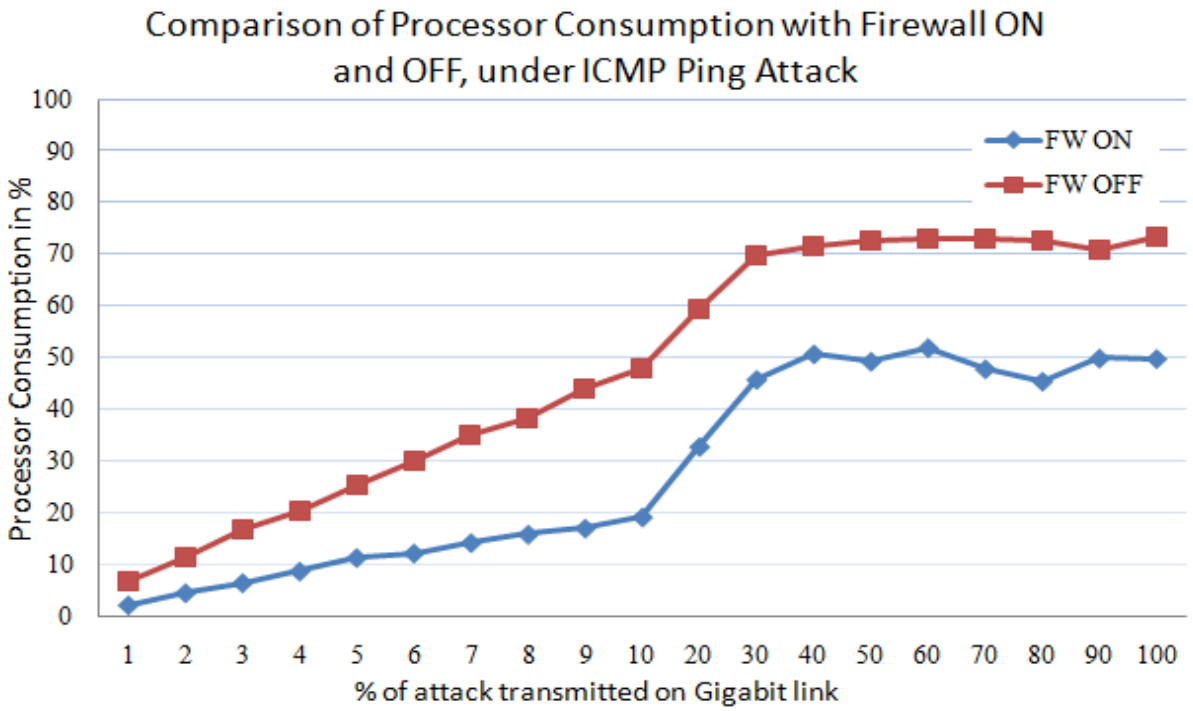



**Figure 2.10:** Comparison of processor consumption by ICMP Ping-Flood Attack on Windows Server 2003 with Firewall OFF and Firewall ON

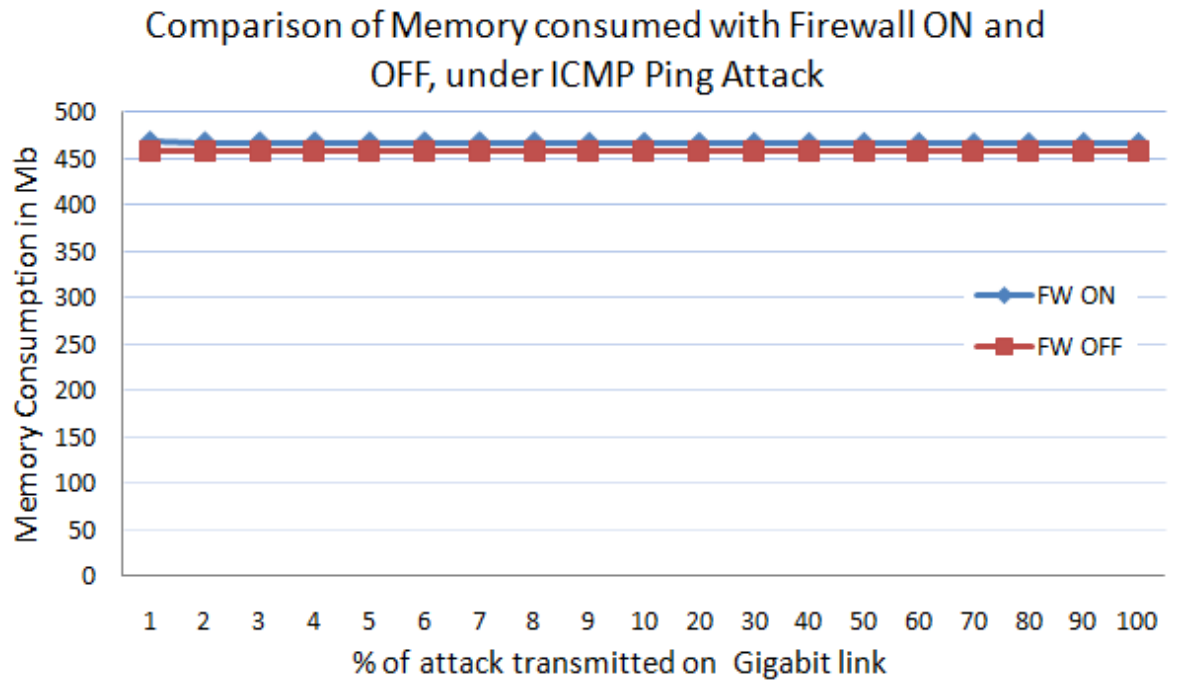



**Figure 2.11:** Comparison of memory consumption by ICMP Ping-Flood Attack on Windows Server 2003 with Firewall OFF and Firewall ON

The reason behind the maximum consumption of 73% processor resources at the time no protection enabled on firewall is due to the maximum of 160,000 ICMP Echo request packets received by the Server from the attacker which need to process all those packets, and reply with Echo replies (Fig 2.12 and Fig 2.13). By allowing all the incoming connections by the firewall and replying to the datagram's received by the server, server consumes processor resources, and also the bandwidth. This consumption of processor and bandwidth to the dangerously peak levels can lead to the Denial of Service attack, which may results in no services to the legitimate users.

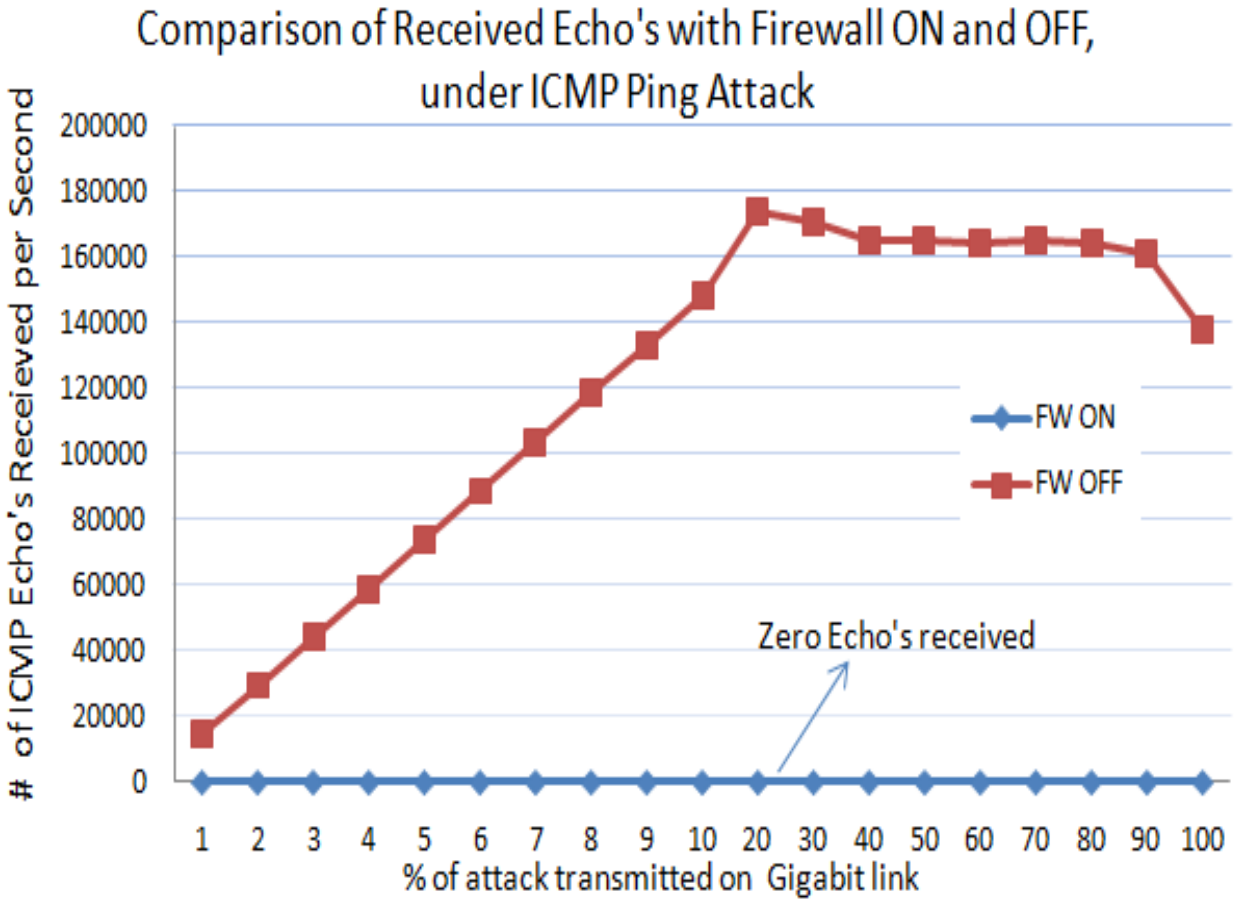



**Figure 2.12:** ICMP Echo Requests received at the time ICMP Ping-Flood Attack on Windows Server 2003 compared with Firewall OFF and Firewall ON

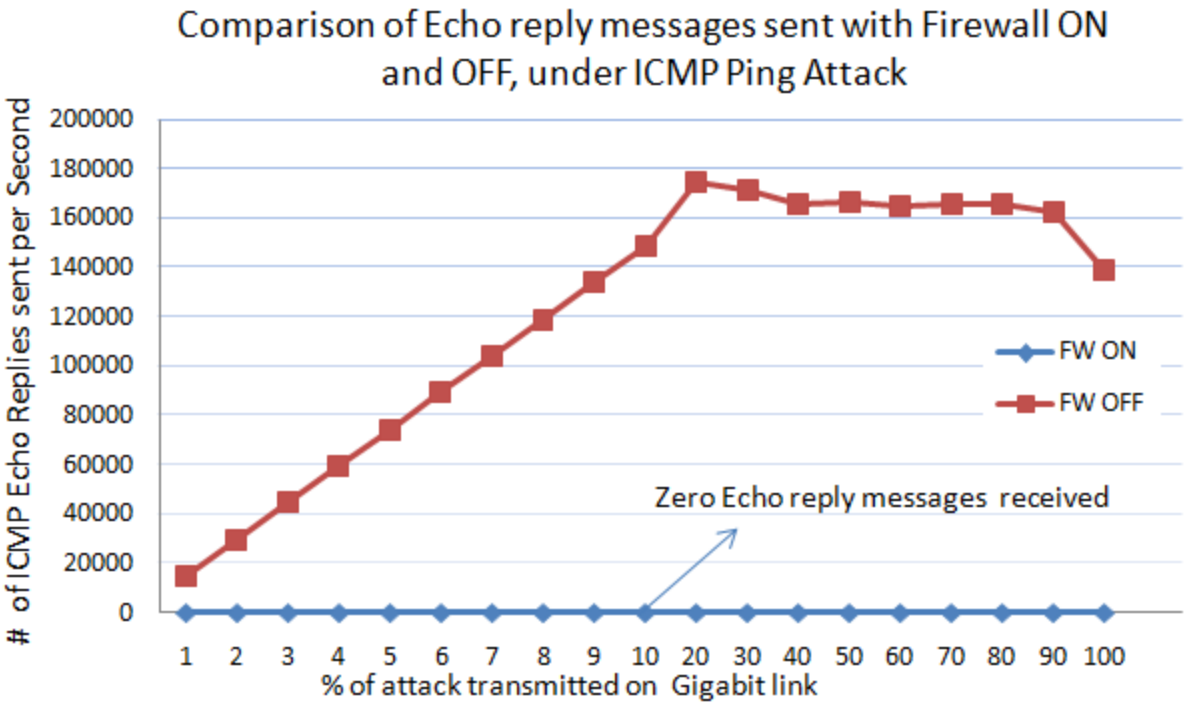
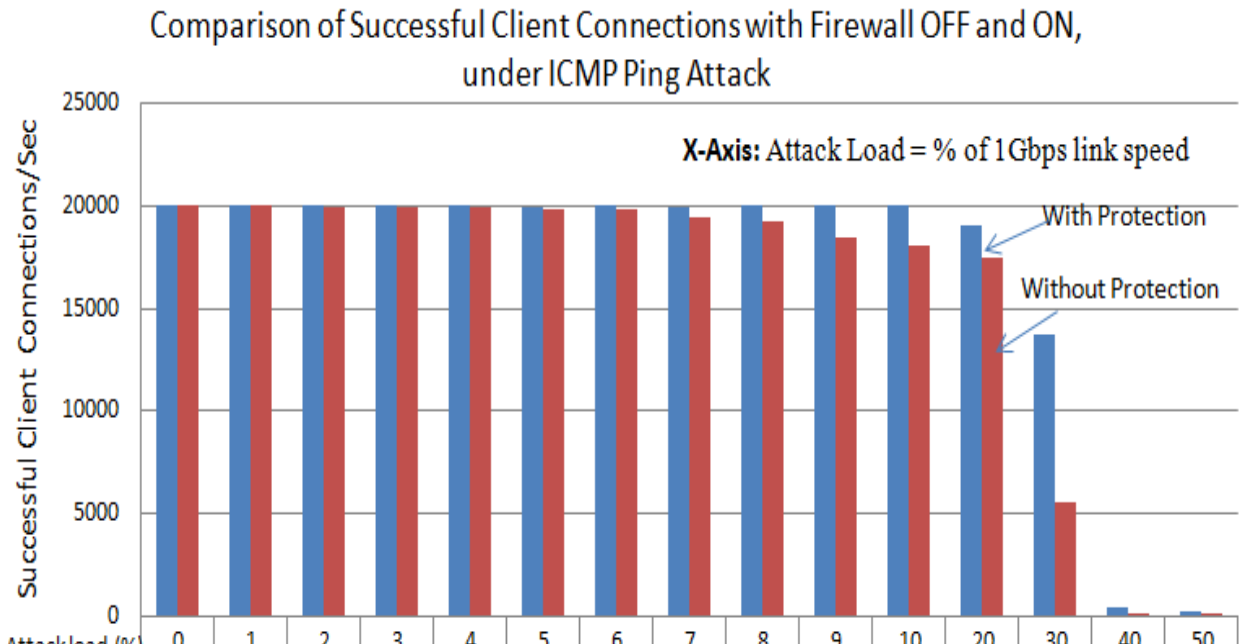



**Figure 2.13:** ICMP-Echo replies sent by server at the time of ICMP Ping-Flood Attack on Windows Server 2003 with Firewall OFF compared with Firewall ON

The reason behind the maximum consumption of 50% processor when the protection on Firewall is enabled at 20Mbps of attack load is due to receiving the echo requests sent by the attacker, process all the packets, and then needs to drop them if the packets reached the server are blocked by the access list maintained by the firewall. Because of dropping all the received ICMP packets the server didn't even recognize them as echo request, and so no echo replies were sent to the source address from which the server receives the echo requests. The processor is consumed less compared to the case when the Firewall is disabled to the configuration when allowing all the connections towards the server. The bandwidth resources and some of the processor resources are consumed in processing and dropping the packets that may result in denial of service for legitimate users.

In the Internet, when the legitimate users are receiving service from the server, and at the same time if the ICMP Ping-Flood attack is launched on it, then how is this attack traffic influence the legitimate users, which resembles the situation of real time attack on a busy Web server (Fig. 2.14). HTTP legitimate traffic are 20,000 Client connections per Second is maintained towards the server, which is simulated as the traffic coming from different users (Different IP address) all-around the Internet, and the attack traffic of different loads in a range of 10Mbps to 1Gbps is directed towards the server serving the legitimate traffic. The comparison of successful Client connections formed between the server and the legitimate users at the time of attack, at varying loads and with two cases; firewall protection enabled and disabled are observed from Fig. 2.14.




| Attack load (%) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 20 | 30 | 40 | 50 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FW ON | 20000 | 19998 | 19998 | 20000 | 20000 | 19994 | 20000 | 19988 | 20000 | 19998 | 19999 | 19071 | 13776 | 440 | 241 |
| FW OFF | 20000 | 20000 | 19981 | 19920 | 19910 | 19890 | 19874 | 19496 | 19276 | 18514 | 18048 | 17498 | 5516 | 30 | 30 |

**Figure 2.14:** Successful client-connections/Second formed at the time of type ICMP-Ping Flood Attack on Windows Server 2003 with Firewall OFF compared with Firewall ON

From figure 2.14, it is observed that the successful legitimate connection are formed with the server are 20,000 per second with no attack traffic. However this number decreases with the increase of the ICMP-Flood attack load, no client connections could be established when the attack load was increased to 40% (400Mbps) of the attack load with no protection enabled on the firewall. When the server is protected with the protection on the firewall blocking all the illegitimate connections, leads to good improvement in the successful connections compared to the case with no protection. However the successful connections are brought down to less than 500 connections at 50% (500Mbps) of attack load. The total number of connections are 18,041 in case with no protection and with protection it is 19,999 at 10% (100Mbps) attack load and at 30% (300Mbps) attack load successful connections are brought down to 5,516 with no protection, which are more lesser when compared to the case when protection is enabled, which is recorded as 13,777 connections per second.

From these two cases we observe that Windows server 2003 is defending well with protection enabled on the firewall, when compare with the protection disabled and allowing all the incoming connections, at the time of ICMP Ping-Flood attack, however. At higher loads of ping attack traffic, even with the protection enabled on the firewall blocking all the attack traffic is not able to withstand the attack. Server is not able to serve the legitimate users, resulting in almost less than 500 successful connections at 50% (500Mbps) ICMP-Ping flood attack load.

### 2.3.4 Security Provided by Microsoft Windows Server 2003 under ICMP Land attack

In this case ICMP Echo requests are flooded towards the server, with source and destination IP addresses same as the target victim IP addresses. When the victim receives this Echo request message then, it sends the Echo reply message to the source IP address of the received packet, which is nothing but its own address. The victim receives the Echo reply sent by it-self, which may consume more victim resources. In this process of processing the received packets, and also receiving the sent echo replies and dropping the received echo replies, server consumes its resources. If this type of land attack traffic is flooded with a barrage of such requests, all the critical system resources such as processor, memory and bandwidth can be consumed resulting in denial of service. This ICMP Land Attack traffic of layer - 3 is sent to server, making it to process and reply itself to all echo request received by the server and consumes all the critical resources on the it, that need to allocated for legitimate users, leads to DoS attack which results in no limited resources for the legitimate users, for their services.

In this case ICMP Land attack traffic at varying loads from 10Mbps to 1Gbps, is sent towards server deploying Windows Server 2003 Operating System on it, where results of processor utilization, memory utilization, packets received and packets sent are observed, compared under two cases; first is without protection from Firewall allowing all the incoming connections, and second is with protection from firewall, blocking all the unused or unsafe connections are blocked in reaching the server. It is observed that Windows 2003 server is consuming a maximum of 37% of processor resources and with memory resources consuming 460Mb constantly in the case of no protection from firewall, and with protection enable on the firewall. The processor is consumed a maximum of 15% with memory at 460Mb all over the experiment in the case of protection enabled on the firewall (Fig’s 2.15 and 2.16).

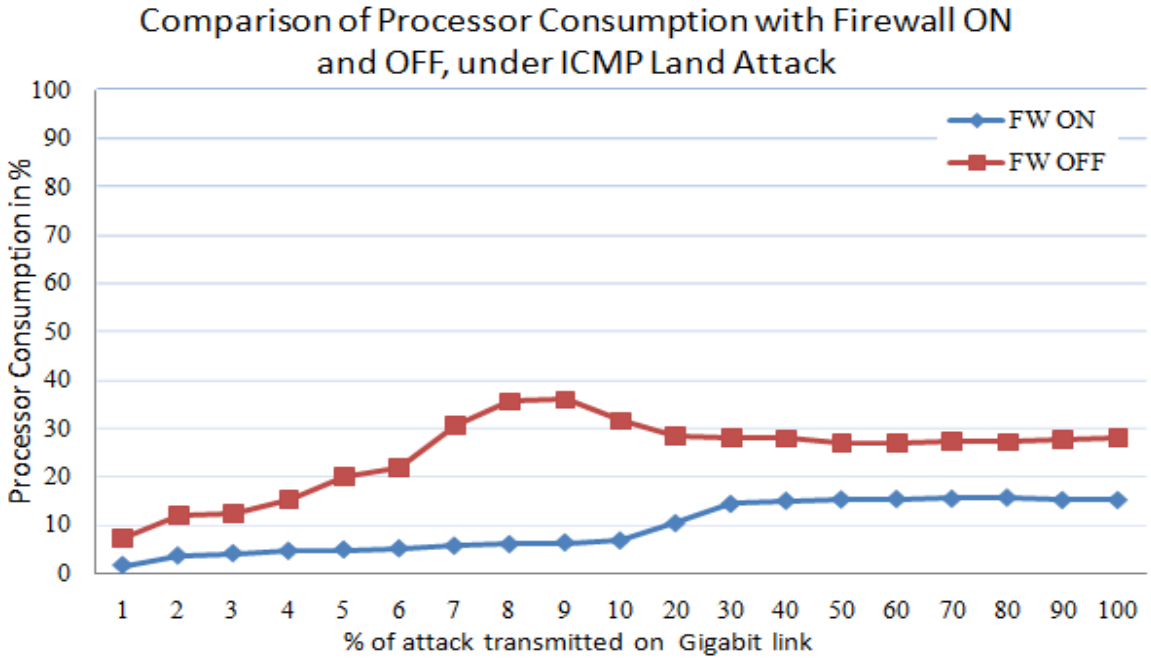



**Figure 2.15:** Comparison of processor consumption by ICMP Land Attack on Windows Server 2003 with Firewall OFF and Firewall ON

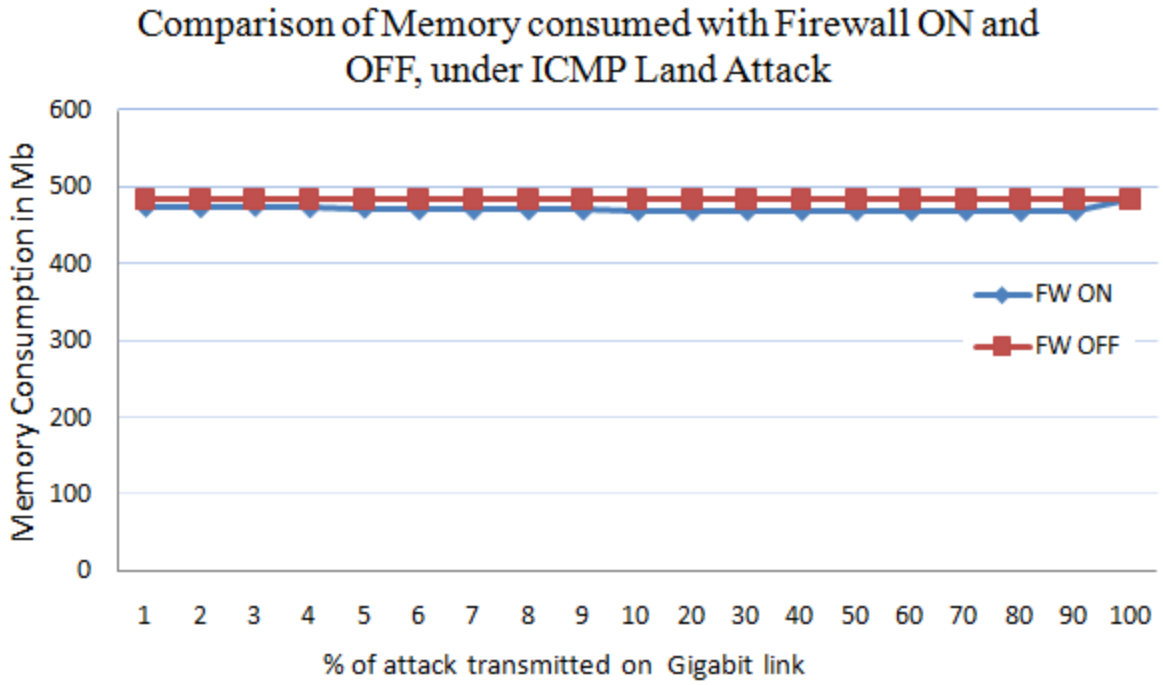



**Figure 2.16:** Comparison of memory consumption by ICMP Land Attack on Windows Server 2003 with Firewall OFF and Firewall ON

The reason behind the maximum consumption of 37% processor without protection enabled on firewall at 20% (200Mbps) Land attack load is due to the maximum of 1,60,000 ICMP Echo request packets received by the Server. The server processes all these packets, replying them with Echo replies, which may again return to the server, due to the land attack packets. By allowing all the incoming connections by the firewall such as land attack packets, and packets forwarded to the ports that are not in use, may lead to the Denial of Service attack. (Fig's 2.17 and 2.18)

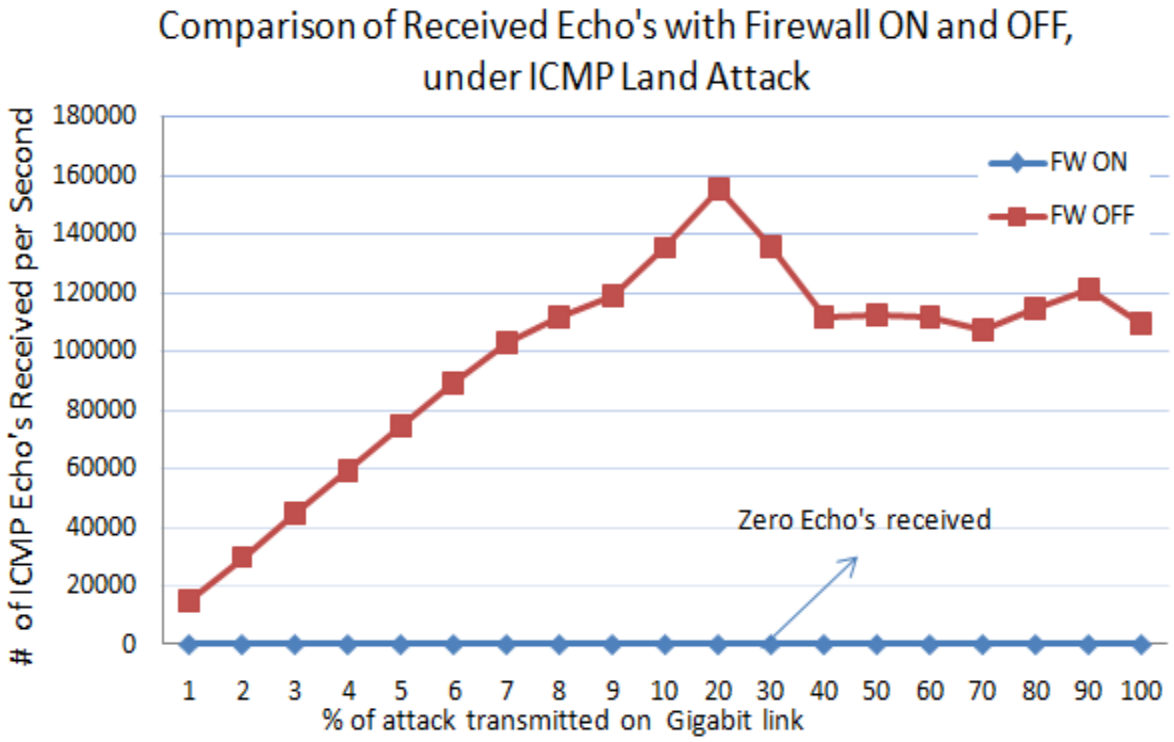



**Figure 2.17:** ICMP Echo Requests received at the time of ICMP Land Attack on Windows Server 2003 compared with Firewall OFF and Firewall ON

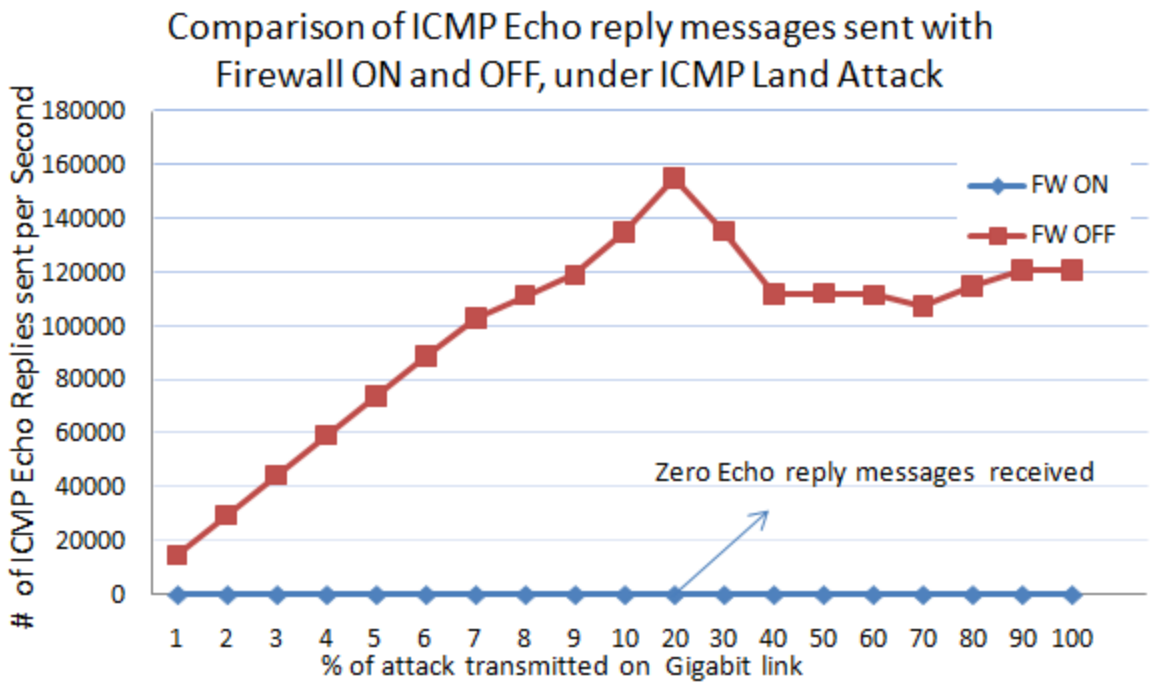
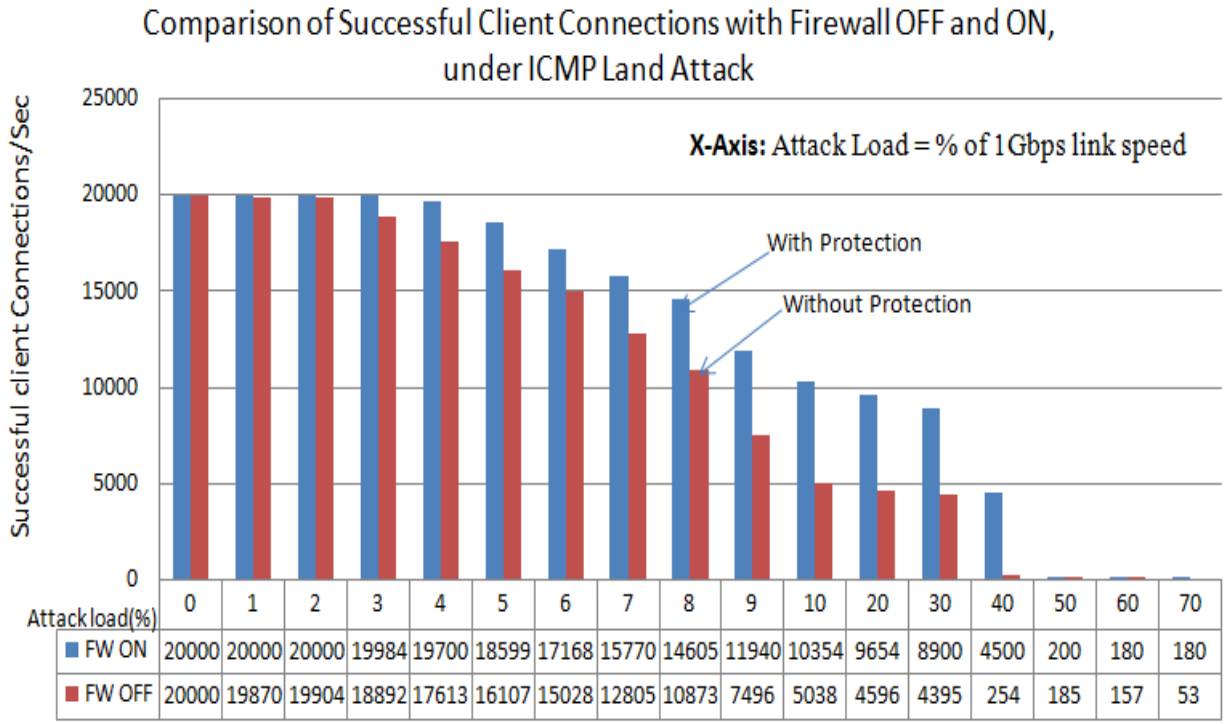



**Figure 2.18:** ICMP-Echo replies sent at the time of ICMP Land Attack on Windows Server 2003 with Firewall OFF compared with Firewall ON

However the reason behind the consumption of 15% processor when the protection on Firewall is enabled is due to, receiving the echo request sent by the attacker. This is because, the server needs to process all the packets and needs to drop them if the packets reached the server are blocked by the access list maintained by the firewall. The server didn't even recognize the received packets as echo requests and so no echo replies are even send to the source address from which the server receives the echo requests. Processor is consumed less compared to the case when the Firewall is disabled, allowing all the connections towards the server. However, the bandwidth resources and some of the processor resources are consumed in processing and dropping the packets may results in denial of service for legitimate users (Fig's 2.17 and 2.18).

In the Internet, when the legitimate users are receiving service from the server and if ping attack is launched on the server, then how is this attack influence the legitimate users? This resembles the situation of real time environment with a busy server (Fig. 2.19). Where HTTP legitimate traffic with 20,000 Client connections/Sec was maintained towards the server, which are simulated as the traffic coming from different users (Different IP address) all-around the Internet. The attack traffic of different loads in a range of 10Mbps to 1Gbps is directed towards the server serving the legitimate traffic. The comparison of successful Client connections formed between the server and the legitimate users at the time of attack, at varying loads and with two cases firewall protection enabled and disabled are observed (Fig. 2.19).




| Attack load(%) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 20 | 30 | 40 | 50 | 60 | 70 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FW ON | 20000 | 20000 | 20000 | 19984 | 19700 | 18599 | 17168 | 15770 | 14605 | 11940 | 10354 | 9654 | 8900 | 4500 | 200 | 180 | 180 |
| FW OFF | 20000 | 19870 | 19904 | 18892 | 17613 | 16107 | 15028 | 12805 | 10873 | 7496 | 5038 | 4596 | 4395 | 254 | 185 | 157 | 53 |

**Figure 2.19:** Successful client Connections/Second formed at the time of type ICMP-Land Attack on Windows Server 2003 with Firewall OFF compared with Firewall ON

From Fig. 2.19, it was observed that the successful legitimate connection are formed with the server by legitimate users are 20,000 per second with no attack. However this number

decreases with the increasing of the ICMP-Land attack load and resulting in less than 300 connections per second at 40% (400Mbps) of the attack load with no protection enabled on the firewall and when the server is protected with the protection on the firewall blocking all the illegitimate connections leads to improvement in the successful connections compared to the case with no protection, however the successful connections are brought down to less than 300 connections at 50% (500Mbps) of attack load. The total number of connections are 5,038 in case with no protection and with protection it was 10,354 at 10% (100Mbps) Land attack load and at 30% (300Mbps) attack load successful connections are brought down to 4,395 with no protection, which are more lesser to the case when protection was enabled which recorded as 8,900 connections per second.

From these two cases we observe that Windows server 2003 was defending good with protection enabled on the firewall, when compare with the protection disabled and by allowing all the incoming connections, at the time of ICMP Ping-Flood attack, however at higher loads of attack traffic, even with the protection enabled on the Firewall, blocking all the illegitimate traffic was not able to withstand the attack traffic and was not able to serve the legitimate users, resulting in almost less than 300 successful connections at 50% (500Mbps) attack load.

## 2.4 Evaluation of Microsoft Windows Server 2008 under common Denial of Service attacks

### 2.4.1 Maximum number of stable connections that can be form with the server

To find the maximum number of stable connections that can be formed with the server, the system with Web server installed on it was send continuous HTTP request from different clients with different source IP address and source port numbers, from Internet. At this time, no attack traffic was sent towards the server and the server was not stressed with any other service. This experiment was continued for 19,000Sec to observe the stable connections maintained by the server.

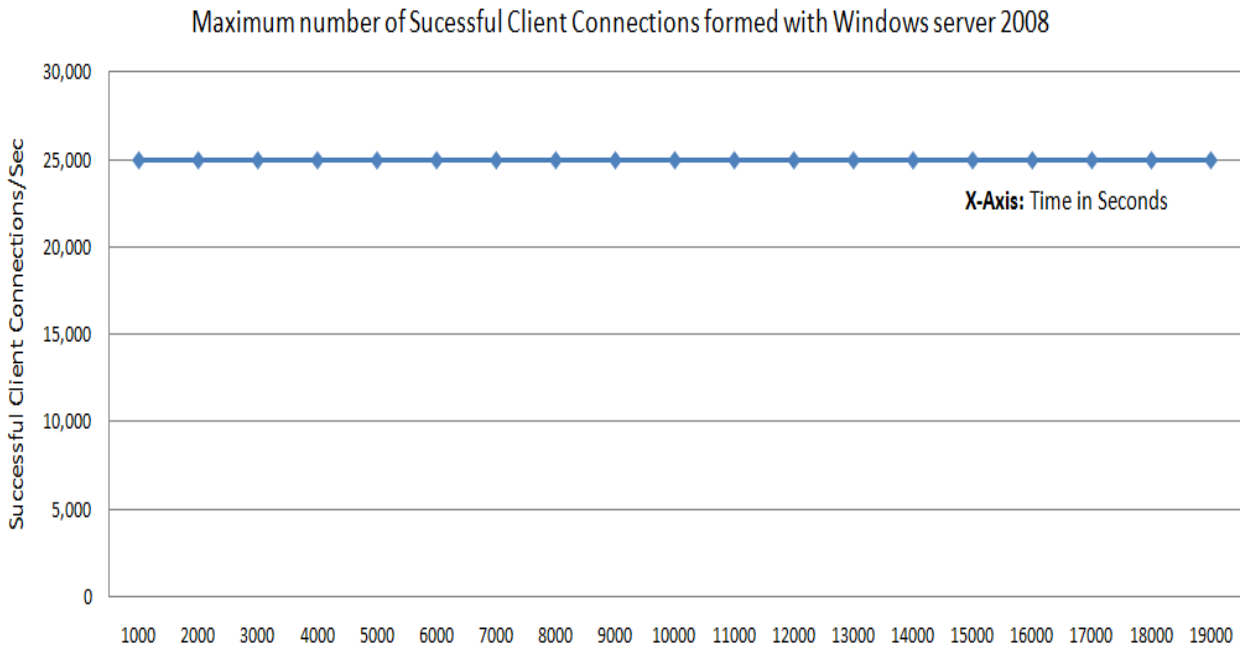



**Figure 2.20:** Maximum number of successful connections formed with Windows Server 2008

From the Fig. 2.20, the maximum number of stable client connections formed by the Web-Server with the legitimate clients are 25,000.

### 2.4.2 Security Provided by Microsoft Windows Server 2008 under TCP-SYN attack

At first, no legitimate traffic are send towards the server and only attack traffic was send in different loads. The TCP-SYN attack traffic at varying loads are sent towards the server, which consumes the resources on the server, in processing them before establishing the complete connection, and just by receiving the SYN packets. The server will reserve some resources for the clients who requested to form new connection by sending the SYN packets. So, this can lead to the consumption of all the critical resources on the Web server, in less time by flooding small amount of SYN attack traffic.

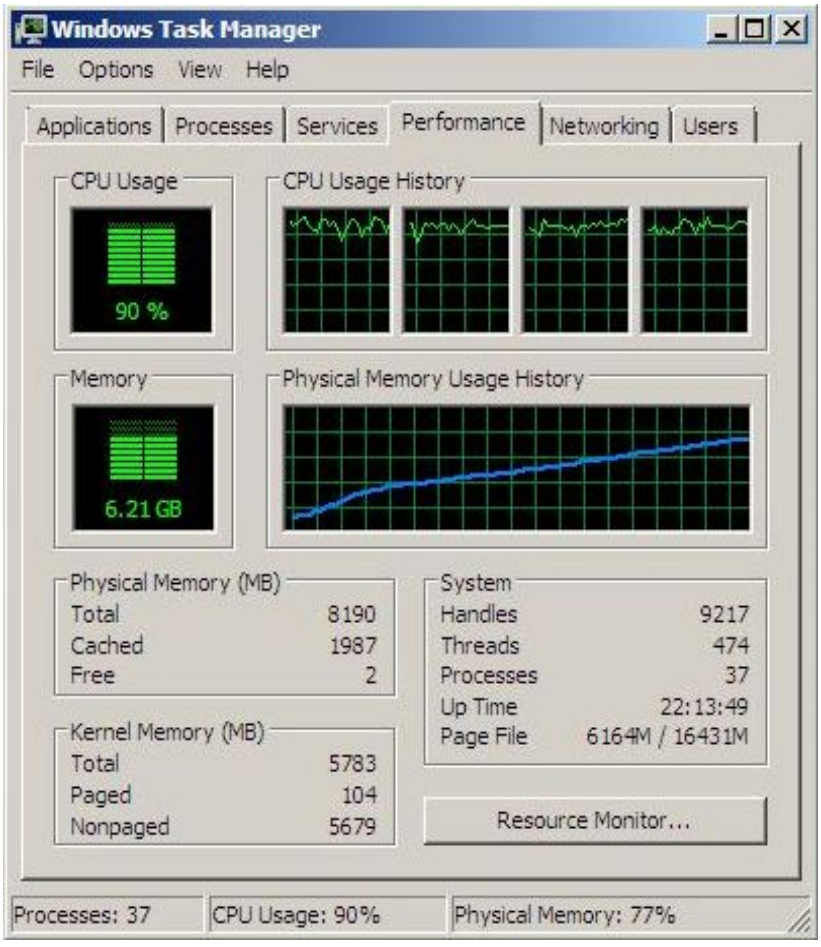



**Figure 2.21:** Snapshot of the memory depletion at 6Mps Attack Load on Server 2008

From the Fig. 2.21, it is observed that the memory was consumed up-to 6.21 GB of the total 7 GB memory within seconds, at 6Mbps SYN attack load. But the processor was not so influenced with the attack load, which varies from 60% to 90% of the total processor. The server at this point when the memory was consumed to the peak point of 6.21 GB remains freeze and even we are not able to move the mouse.

How SYN attack traffic effects in the real time, can be seen when the legitimate traffic was maintained at 25,000 connections per second and the SYN attack traffic of differ loads are directed towards that server. So, in this case, we sent the legitimate HTTP traffic from different clients having individual IP address, initiated from Internet towards the targeted Web Server, which is configured on the Microsoft Windows Server 2008 (SP-1) resulted in maximum of 25,000 connections per second, without any attack towards the server. The TCP-SYN attack traffic, where flood of SYN packets are sent towards the server at different loads, and at these different loads the processor consumption, memory consumption, number of attack packets received and packets sent by the server, as reply for the received packets are observed and plotted, which helps in understand the behavior of the server at the time of TCP-SYN attack.

When the TCP-SYN attack was sent on to the server, then the SYN packets which are sent towards the server will not only consume resources for processing those packets, but also reserve some recourse on the server to maintain connection between the server and client which helpful in forming a reliable data transfer.

In the results (Fig. 2.22), it is found that Microsoft Windows Server 2008 with service pack -1 on it is crashed at 6 Mbps SYN attack load, and this is due to the depletion of memory as explained in the previous section.

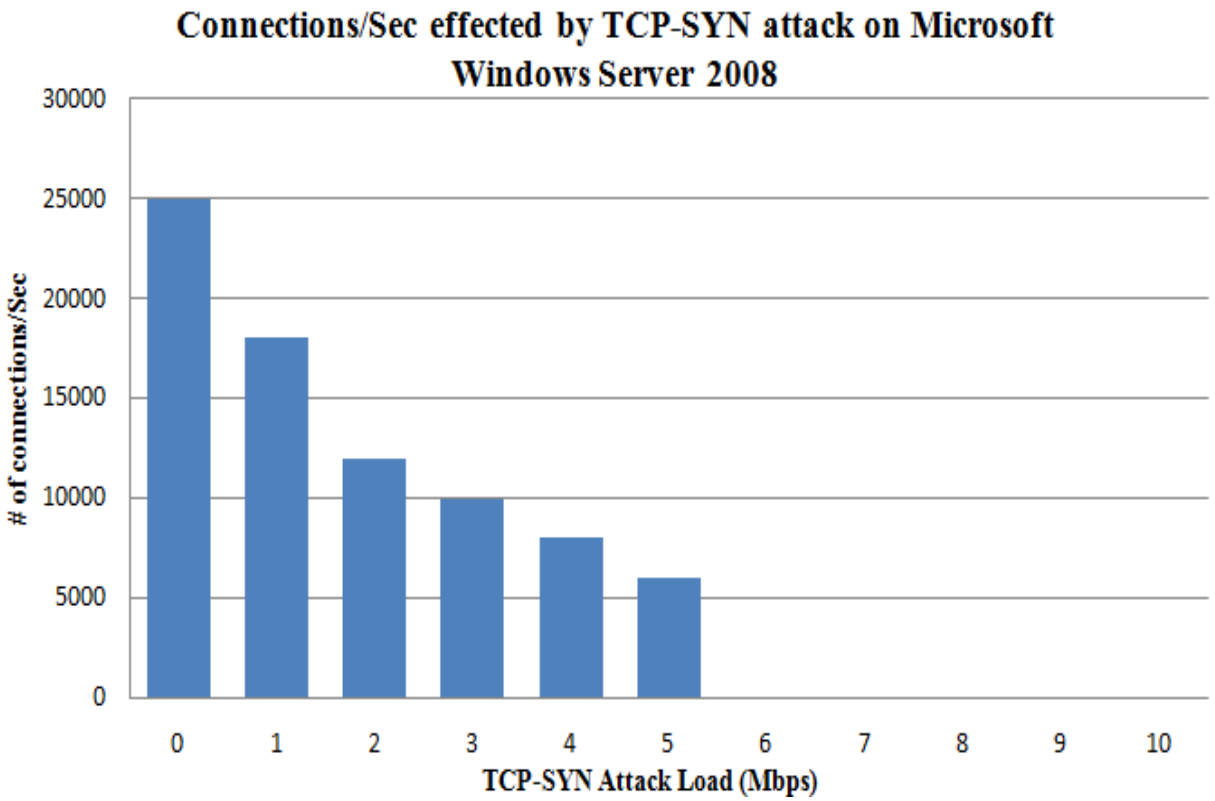



**Figure 2.22:** Number of successful client connections per second under TCP-SYN attack load

From Fig. 2.22, it is observed that the server having 25,000 connections per second at no attack load, drops to zero connection when the attack traffic reached the server with 6Mbps load, that takes few seconds to consume all the memory resources and bring down the server, where no legitimate users are able to have service from server which is crashed and not even able to move the mouse.

### 2.4.3 Security Provided by Microsoft Windows Server 2008 under UDP-Flood attack

In this case barrage of UDP packets are sent to random ports of server requesting for a service at that port. If no services are available on that port, then the server sends an ICMP Destination Unreachable message back to the source address on the received packets. In this process of processing the received packets, server consumes some of its resources. If it is flooded with a barrage of such requests all the system resources will be consumed resulting in denial of service.

In this case UDP Flood attack traffic at varying loads are sent towards server deploying Windows Server 2008 Operating System on it, where results of processor utilization, memory utilization and packets received and sent is observed compared under two cases; first is without protection from Firewall, allowing all the incoming connections and second is with protection from firewall, which is the case all the unused or unsafe connections are blocked in reaching the server which may cause damage to the server. It is observed that Windows 2008 server is consuming a maximum of 43% of processor resources and there is no influence with memory resources which stays constantly at 700Mb in the case of no protection from firewall, and the processor is consumed a maximum of 15% with memory at 700Mb all over the experiment in the case of protection enabled on the firewall (Fig. 2.23).

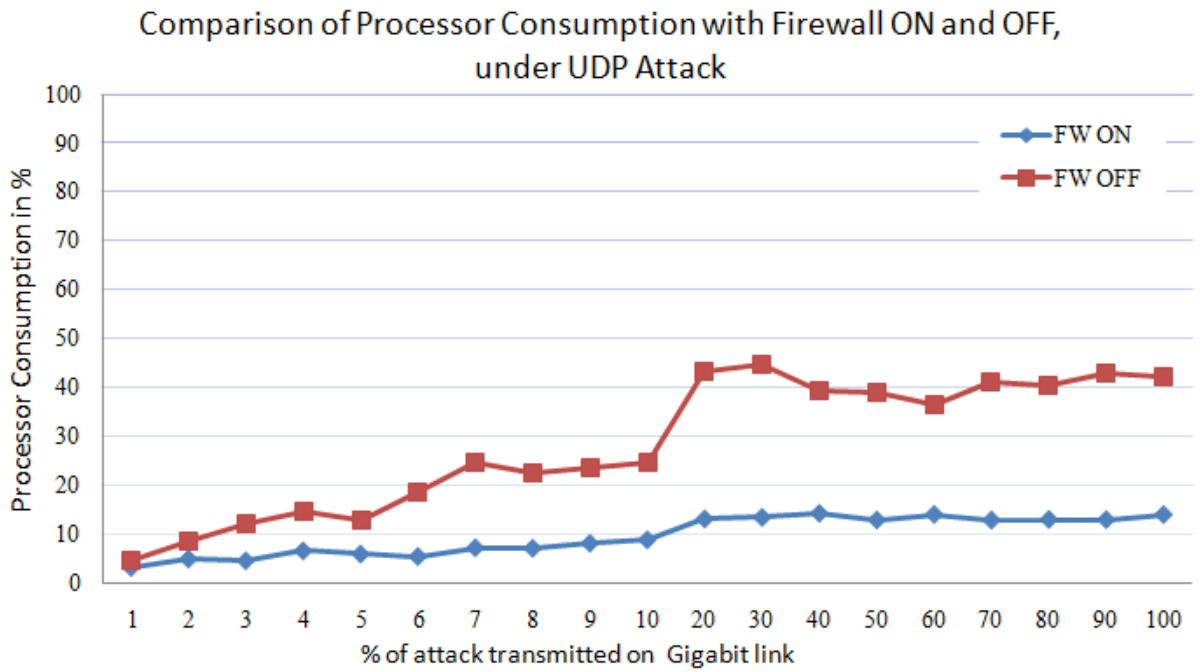



**Figure 2.23:** Comparison of processor consumption UDP-Flood Attack on Windows Server 2008 with Firewall OFF and Firewall ON

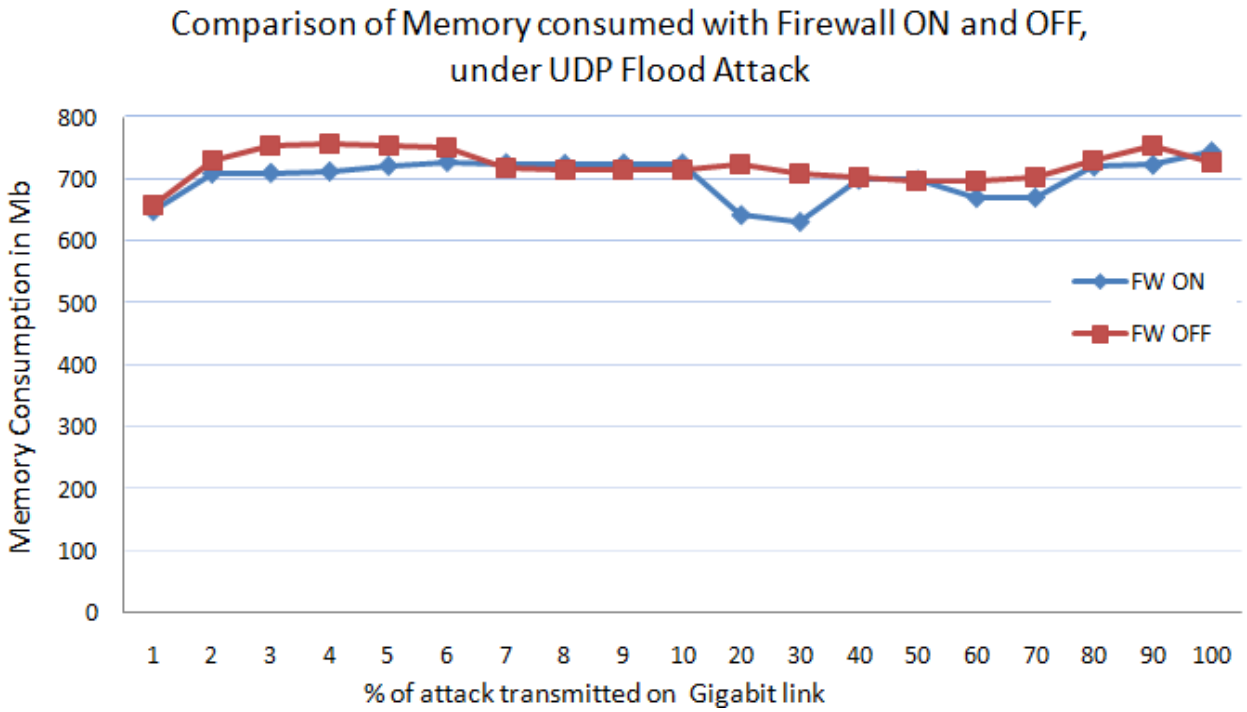



**Figure 2.24:** Comparison of memory consumption UDP-Flood Attack on Windows Server 2008 with Firewall OFF and Firewall ON

The reason behind the consumption of 43% processor is, due to the maximum of 3,50,000 UDP packets received by the server from the attacker and the maximum of 200 ICMP Destination Unreachable Packets sent by the server because of no existing of the application on the port which is requested by attacker (Figures 2.25 and 2.26). This is due to allowing all the incoming connections by the firewall and replying to only 200 datagram's received by the server, consumes processor resources, and also the bandwidth resources, which may results in no services to the legitimate users.

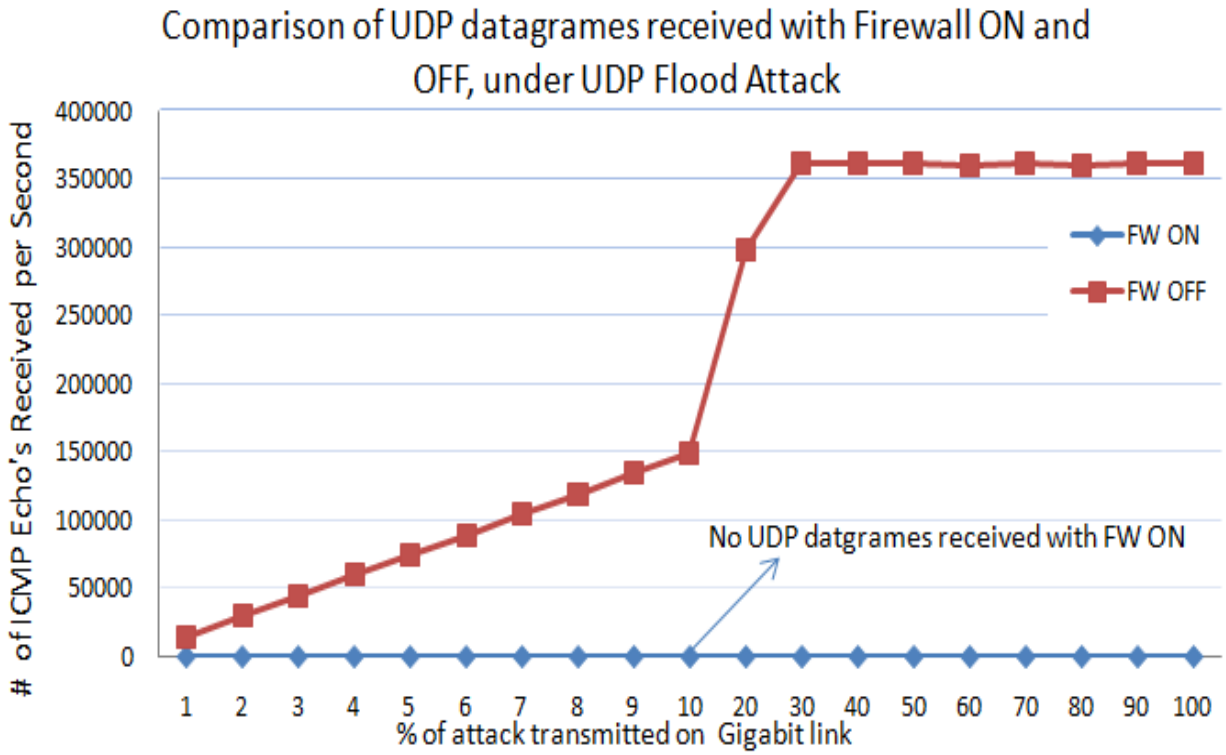



**Figure 2.25:** UDP datagram's received at the time of UDP-Flood Attack on Windows Server 2008 compared with Firewall OFF and ON

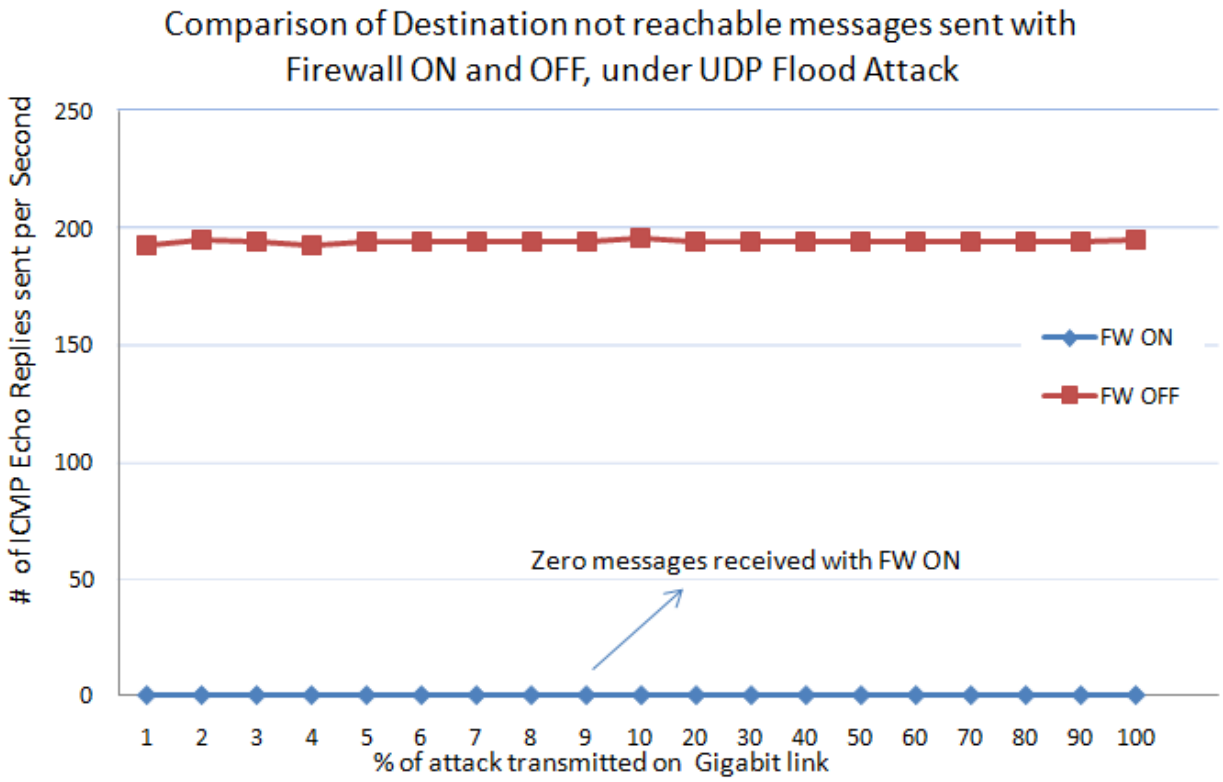
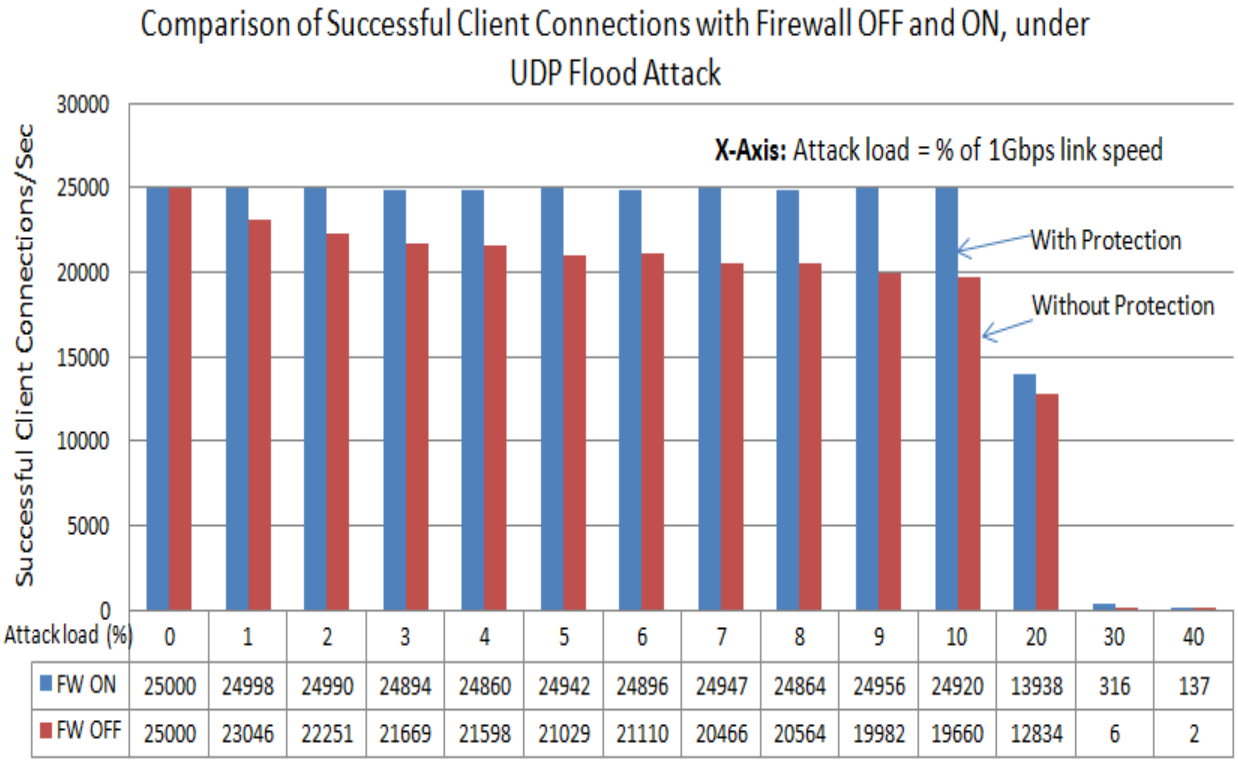



**Figure 2.26:** ICMP-Destination unreachable packets sent at the time of UDP-Flood Attack on Windows Server 2008 with Firewall OFF compared with Firewall ON

However the reason behind the consumption of 15% processor when the protection on Firewall is enabled is due to, no UDP packets received by the Server from the attacker, and the server just drops the received illegitimate traffic, without sending ICMP Destination Unreachable Packets (Fig's 2.25 and 2.26), because of not allowing all the incoming connections by the firewall. So the processor is consumed less compared to the case when the Firewall is disabled, allowing all the connections towards the server. However, the bandwidth resources and some of the processor resources are consumed in processing and dropping the packets may results in denial of service for legitimate users.

In the Internet, when the legitimate users are getting service from the server, and at the same time if the UDP-Flood attack was launched on the server, then how is this attack influence the legitimate users, can be observed from Fig. 2.27, where HTTP legitimate traffic with 25,000 Client connections/Sec are maintained towards the server, which was simulated as the traffic coming from different users (Different IP address) all-around the Internet, and the attack traffic of different loads in a range of 10Mbps to 1Gbps is directed towards the server serving the legitimate traffic. The comparison of successful Client connections formed between the server and the legitimate users at the time of attack at varying loads and with two cases; firewall protection enabled and disabled are observed (Fig. 2.27).




| Attack load (%) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 20 | 30 | 40 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FW ON | 25000 | 24998 | 24990 | 24894 | 24860 | 24942 | 24896 | 24947 | 24864 | 24956 | 24920 | 13938 | 316 | 137 |
| FW OFF | 25000 | 23046 | 22251 | 21669 | 21598 | 21029 | 21110 | 20466 | 20564 | 19982 | 19660 | 12834 | 6 | 2 |

**Figure 2.27:** Successful client connections/Second formed at the time of UDP-Flood Attack on Windows Server 2008 with Firewall OFF compared with Firewall ON

From Fig. 2.27, it is observed that the successful legitimate connection are formed with the server by legitimate users are 25,000 per second with no attack traffic. However, this number decreases with the increasing of the UDP-Flood attack load and resulting in almost zero legitimate connection at 30% (300Mbps) of the attack load with no protection enabled on the firewall. When the server is protected with the protection on the firewall blocking all the illegitimate connections leads to good improvement in the successful connections compared to the case with no protection, however the successful connections are brought down to less than 150 connections at 40% (400Mbps) of attack load. The total number of connections are 19,660 in case without protection, and with protection it was 24,956 at 10% (100Mbps) attack load and at 20% (200Mbps) attack load successful connections are brought down to 12,834 with no protection, which are more lesser to the case when protection was enabled which recorded as 13,938 connections per second.

From these two cases we observe that Windows server 2008 is defending well with protection enabled on the firewall, when compare with the protection disabled and by allowing all the incoming connections, at the time of UDP-Flood attack, however at higher loads of attack traffic, even with the protection enabled on the Firewall, blocking all the illegitimate traffic is not able to withstand the attack traffic and is not able to serve the legitimate users, resulting in almost less than 150 successful connections at 400Mbps attack load.

### 2.4.4 Security Provided by Microsoft Windows Server 2008 under ICMP PING-Flood attack

In this case ICMP Echo requests are flooded towards the server requesting for a Ping reply, which states the availability of that system in the network. In this process of processing the received packets, server consumes some of its resources. If it is flooded with a barrage of such requests all the critical system resources such as processor, memory and bandwidth will be consumed resulting in denial of service. And this ICMP Attack traffic of layer - 3 is sent to server, making it to process and reply to all echo request received by the server and consuming the resources leads to DoS attack which results in no limited resources for the legitimate users for their services.

In this case ICMP Flood attack traffic at varying loads, from 10Mbps to 1Gbps, was sent towards server deploying Windows Server 2008 Operating System on it, where results of processor utilization, memory utilization and packets received and sent are observed compared under two cases; first is without protection from Firewall, allowing all the incoming connections and second is with protection from firewall, which is the case all the unused or unsafe connections are blocked in reaching the server which may cause damage to the server. It is observed that Windows 2008 is consuming a maximum of 80% of processor resources and the memory resources are also increased with the increase in the attack traffic, which reaches to the peak of 6000Mbps at 1Gbps attack traffic at the time of Firewall disabled, and the processor is consumed a maximum of 70% with memory at 700Mb all over the experiment in the case of protection enable on the firewall (Fig's 2.28 and 2.29)

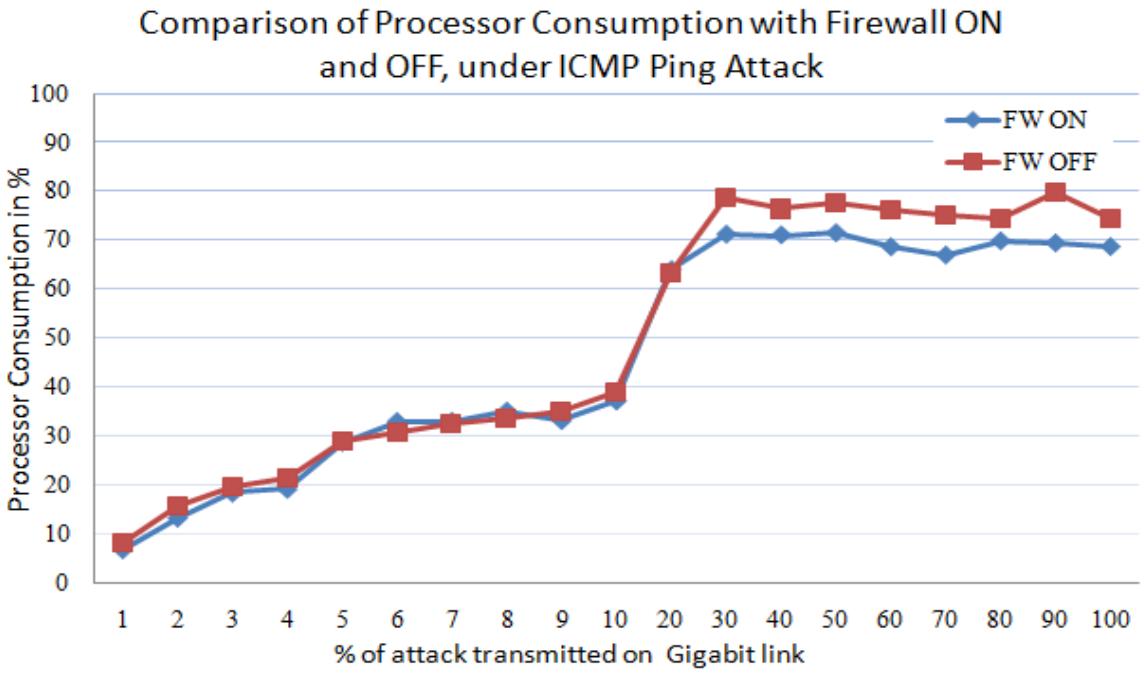



**Figure 2.28:** Comparison of processor consumption by ICMP Ping-Flood Attack on Windows Server 2008 with Firewall OFF and Firewall ON

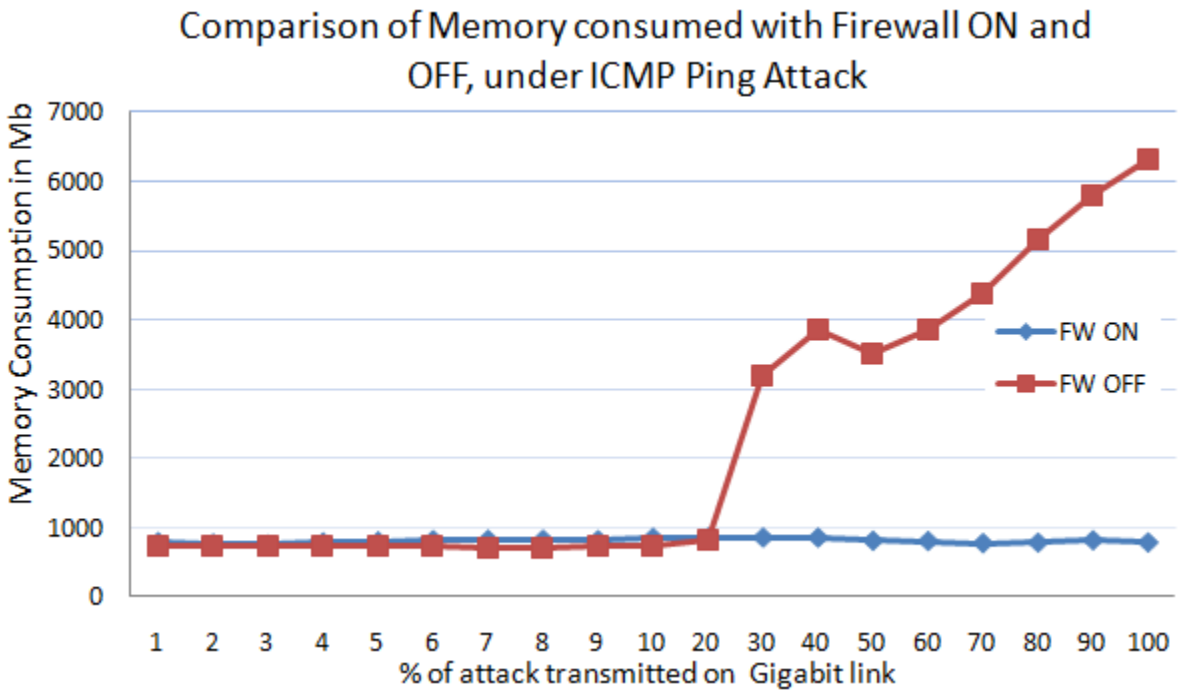



**Figure 2.29:** Comparison of memory consumption by ICMP Ping-Flood Attack on Windows Server 2008 with Firewall OFF and Firewall ON

The reason behind the consumption of 80% processor at the time no protection enabled on firewall is due to the maximum of 350,000 ICMP Echo request packets received by the Server from the attacker and by processing all those packets, replying with Echo replies by the server to the maximum of 170,000 received packets, to state its existence on the network. By allowing all the incoming connections by the firewall and replying to the datagram's received by the server, consumes lot of processor resources, and memory resources along with the bandwidth, and this consumption of processor, memory and bandwidth to the dangerously peak levels can lead to the Denial of Service attack, which may results in no services to the legitimate users (Fig's 2.30 and 2.31).

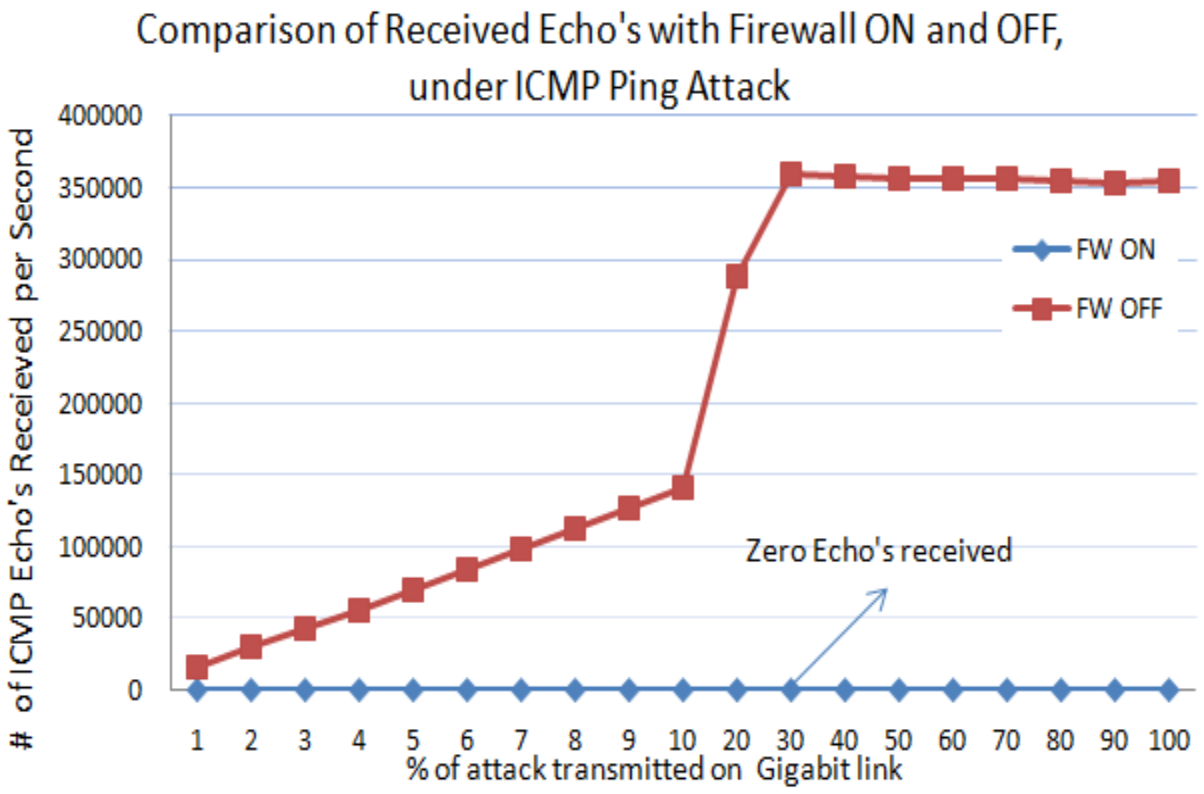



**Figure 2.30:** ICMP Echo Requests received at the time of ICMP Ping-Flood Attack on Windows Server 2008 compared with Firewall OFF and Firewall ON

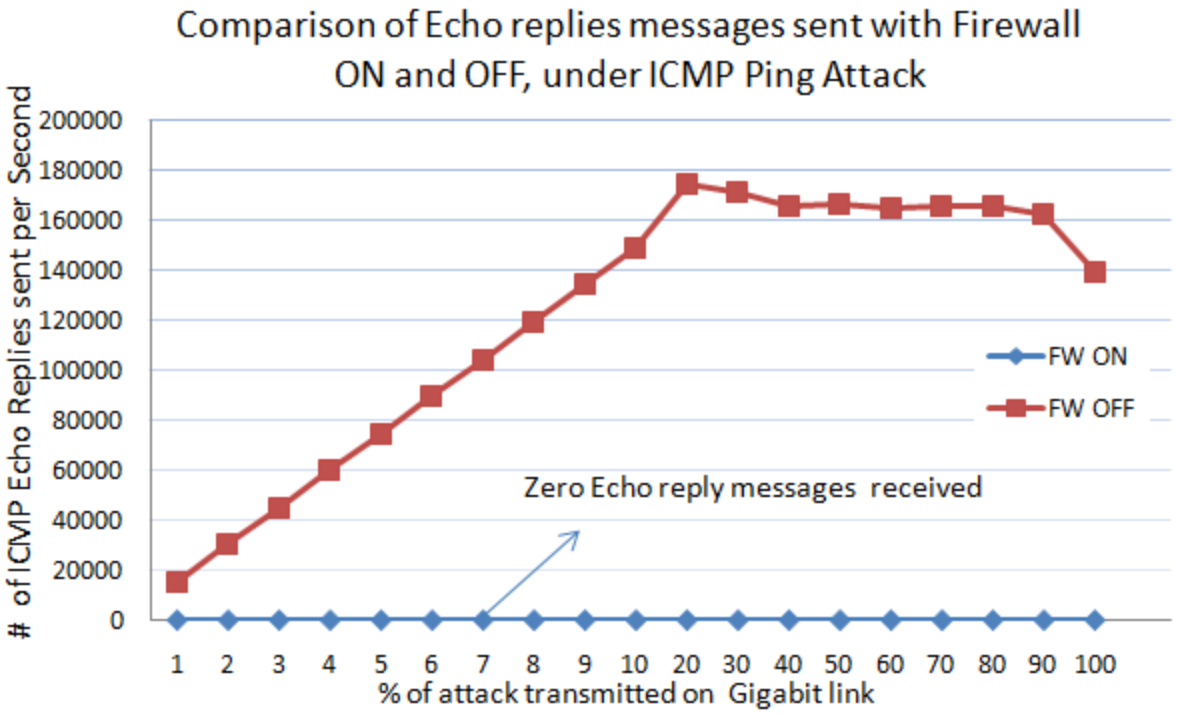
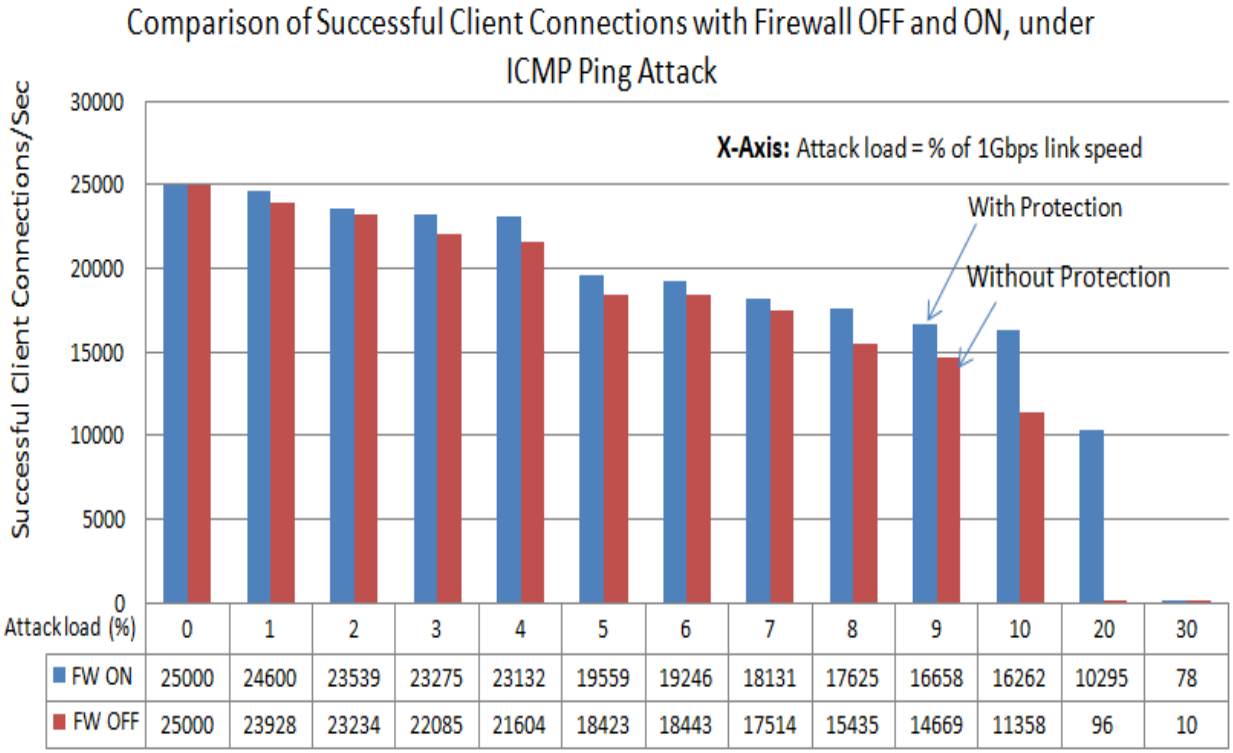



**Figure 2.31:** ICMP-Echo replies sent at the time of ICMP Ping-Flood Attack on Windows Server 2008 with Firewall OFF compared with Firewall ON

However the consumption of 70% processor when the protection on firewall is enabled is due to receiving the echo request send by the attacker (Fig 2.31). This is because server needs to process all the packets and needs to drop them if the packets reached the server are blocked by the access list maintained by the firewall. Because of dropping all the received packets, the server didn't even recognize them as echo request and so no echo replies are even send to the source address from which the server receives the echo requests. So the processor was consumed less compared to the case when the Firewall is disabled, allowing all the connections towards the server. However, the bandwidth resources and some of the processor resources are consumed in processing and dropping the packets may results in denial of service for legitimate users (Fig. 2.30 and 2.31).

In the Internet, when the legitimate users are receiving service from the server, and at the same time if the ICMP Ping-Flood attack is launched on the server, then how is this attack influence the legitimate users, which resembles the situation of real time environment with a busy server, can be observed from Fig. 2.32, where HTTP legitimate traffic with 25,000 Client connections/Sec are maintained towards the server, which is simulated as the traffic coming from different users (Different IP address) all-around the Internet, and the attack traffic of different loads in a range of 10Mbps to 1Gbps is directed towards the server serving the legitimate traffic. The comparison of successful Client connections formed between the server and the legitimate users at the time of attack, at varying loads and with two cases; firewall protection enabled and disabled are observed (Fig. 2.32).




| Attack load (%) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 20 | 30 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FW ON | 25000 | 24600 | 23539 | 23275 | 23132 | 19559 | 19246 | 18131 | 17625 | 16658 | 16262 | 10295 | 78 |
| FW OFF | 25000 | 23928 | 23234 | 22085 | 21604 | 18423 | 18443 | 17514 | 15435 | 14669 | 11358 | 96 | 10 |

**Figure 2.32:** Successful client connections/Second formed at the time of type ICMP-Ping Flood Attack on Windows Server 2008 with Firewall OFF compared with Firewall ON

From Fig. 2.32, it is observed that the successful legitimate connection are formed with the server by legitimate users are 25,000 per second with no attack traffic. However this number decreases with the increasing of the ICMP-Flood attack load and resulting in almost zero legitimate connection at 20% (200Mbps) of the attack load with no protection enabled on the firewall. When the server is protected with the protection on the firewall blocking all the illegitimate connections leads to good improvement in the successful connections compared to the case with no protection, however the successful connections are brought down to less than 100 connections at 30% (300Mbps) of attack load. The total number of connections are 11,350 in case with no protection and with protection it is 16,264 at 10% (100Mbps) attack load and at 20% (200Mbps) attack load successful connections are brought down to 96 with no protection, which are more lesser to the case when protection is enabled which recorded as 10,290 connections per second.

From these two cases, we observe that Windows server 2003 is defending well with protection enabled on the firewall, when compare with the protection disabled, and by allowing all the incoming connections, at the time of ICMP Ping-Flood attack. However at higher loads of attack traffic, even with the protection enabled on the Firewall, blocking all the illegitimate traffic is not able to withstand the attack traffic and is not able to serve the legitimate users, resulting in almost less than 100 successful connections at 300Mbps attack load.

### 2.4.5 Security Provided by Microsoft Windows Server 2008 under ICMP Land attack

In this case ICMP Echo requests are flooded towards the server, with source and destination IP address same as the targeted victim IP address. When the victim received this Echo request message then, it sends the Echo reply message to the source IP address of the received packet, which is nothing but its own address. The victim receives the Echo reply send by himself, which will consume victim resources. In this process of processing the received packets, and also receiving the sent echo replies and dropping the received echo replies, server consumes some of its resources. If it is flooded with a barrage of such requests all the critical system resources such as processor, memory and bandwidth will be consumed resulting in denial of service. And this ICMP Land Attack traffic of layer - 3 is sent to server, making it to process and reply to all echo request received by the server and possibly consuming all the resources leads to DoS attack which results in lack of resources for the legitimate users for their services.

In this case ICMP Land attack traffic at varying loads from 10Mbps to 1Gbps, is sent towards server deploying Windows Server 2008 Operating System on it, where results of processor utilization, memory utilization and packets received and packets sent are observed, compared under two cases first is without protection from Firewall allowing all the incoming connections, and second is with protection from firewall, which is the case all the unused or unsafe connections are blocked in reaching the server which may cause damage to the server. It is observed that Windows 2008 is consuming a maximum of 37% of processor resources and there is no influence with memory resources which stays constantly at 800Mb in the case of no protection from firewall, and with the protection from firewall, the processor is consumed a maximum of 15% with memory at 800Mb all over the experiment in the case of protection enabled on the firewall (Fig’s 2.33 and 2.34).

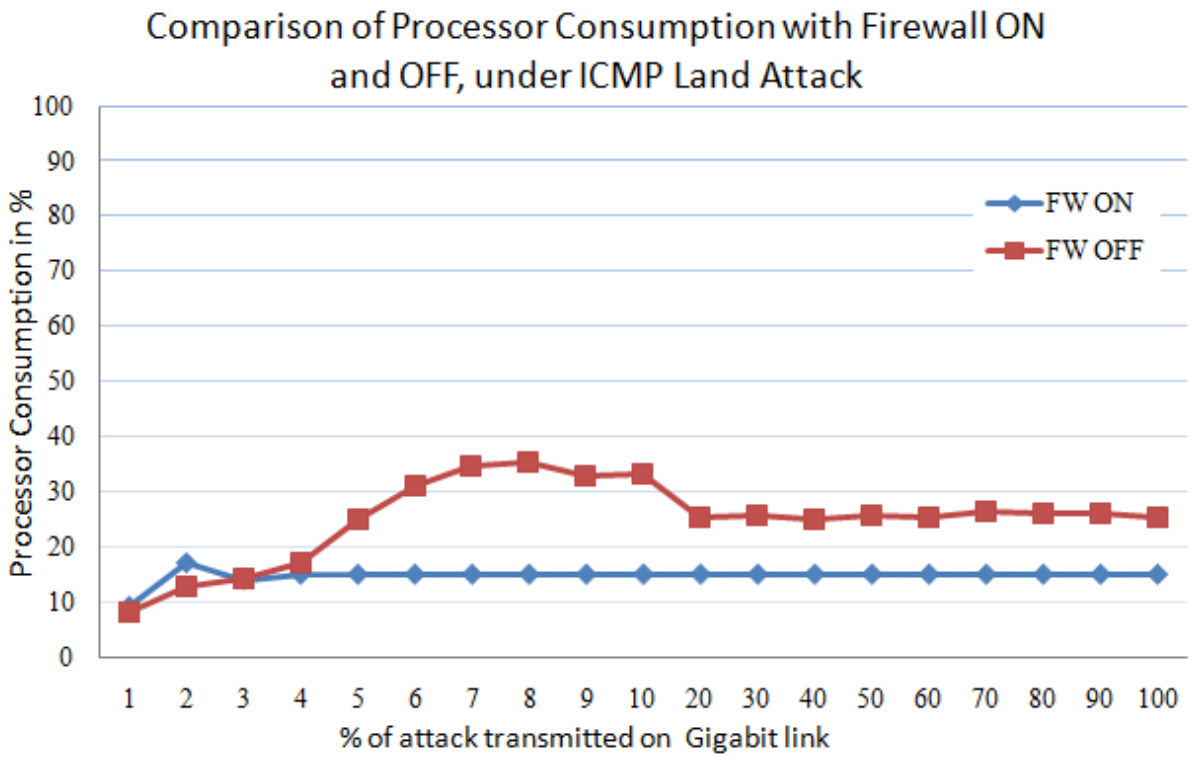



**Figure 2.33:** Comparison of processor consumption by ICMP Land Attack on Windows Server 2008 with Firewall OFF and Firewall ON

The reason behind the consumption of 37% processor at the time no protection enabled on firewall is, due to the maximum of 2,00,000 ICMP Echo request packets received by the Server from the attacker and by processing all those packets, replying with Echo replies by the server, to state its existence on the network. By allowing all the incoming connections by the firewall and replying to the datagram's received by the server, consumes lot of processor resources, and also the bandwidth and this consumption of processor and bandwidth to the dangerously peak levels can lead to the Denial of Service attack, which may results in no services to the legitimate users (Fig's 2.35 and 2.36).

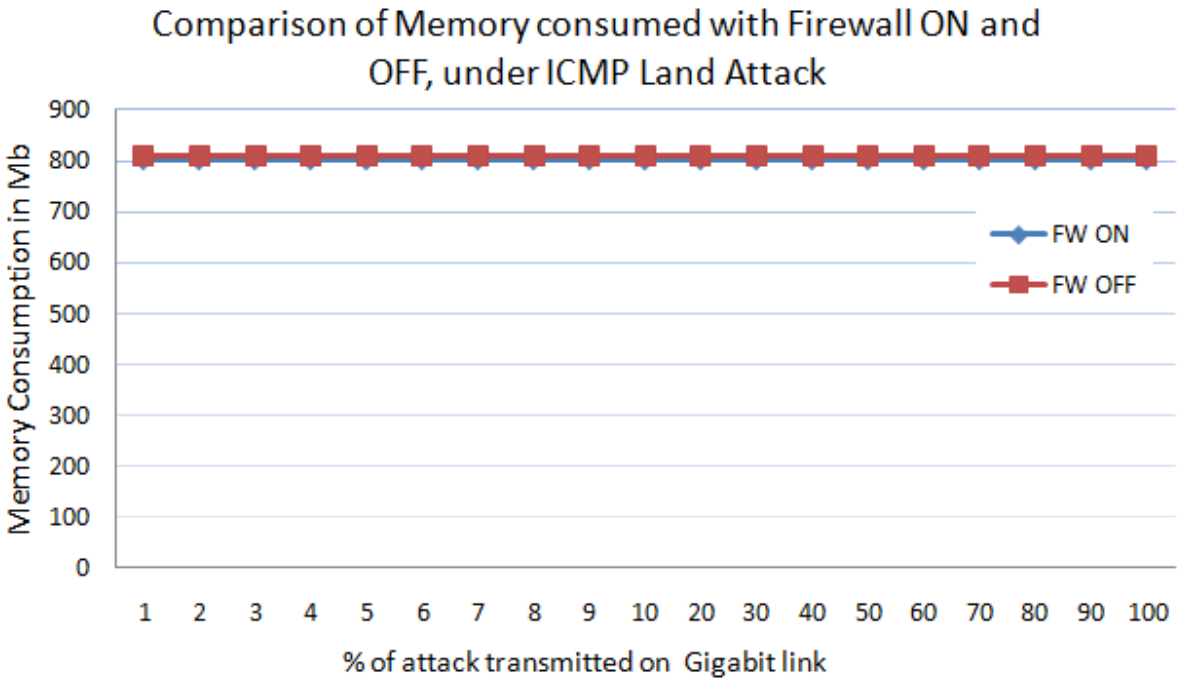



**Figure 2.34:** Comparison of memory consumption by ICMP Land Attack on Windows Server 2003 with Firewall OFF and Firewall ON

However the reason behind the consumption of 15% processor when the protection on Firewall is enabled is due to, receiving the 2,00,000 echo requests send by the attacker, and because the server needs to process all the packets and needs to drop them if the packets reached the server is blocked by the access list maintained by the firewall, and because of dropping all the received packets the server didn't even recognize them as echo request and so no echo replies are even send to the source address from which the server receives the echo requests. So the processor is consumed less compared to the case when the Firewall is disabled, allowing all the connections towards the server. However, the bandwidth resources and some of the processor resources are consumed in processing and dropping the packets may results in denial of service for legitimate users (Fig's 2.35 and 2.36).

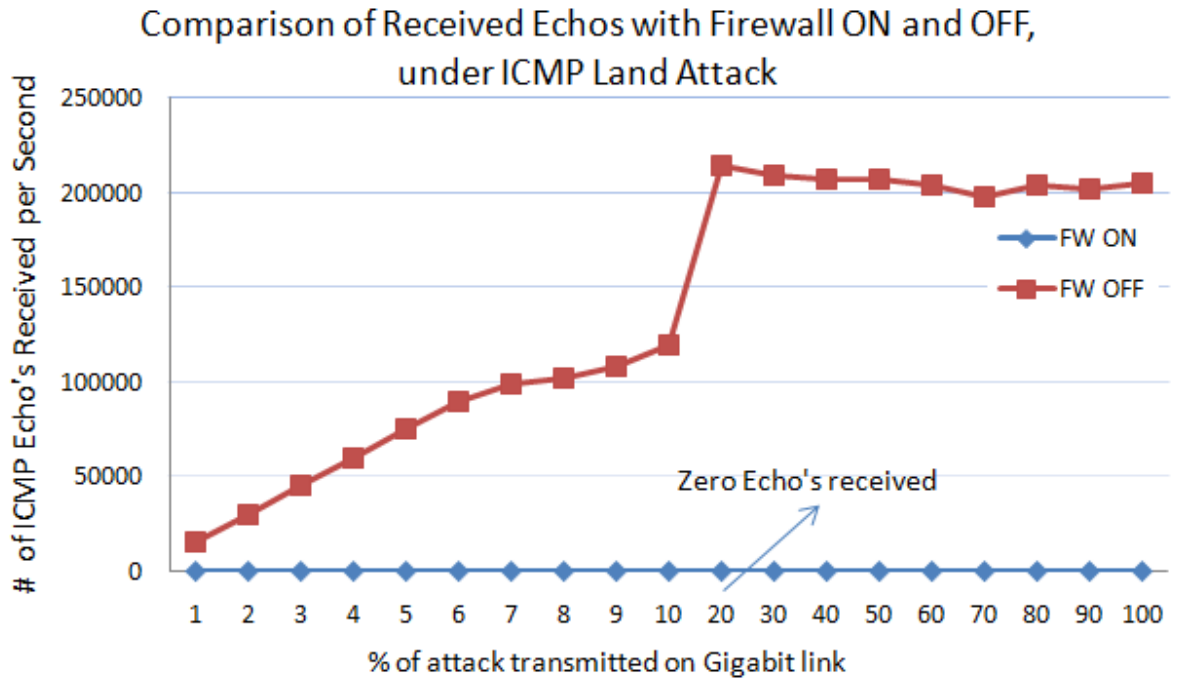



**Figure 2.35:** ICMP Echo Requests received at the time of ICMP Land Attack on Windows Server 2008 compared with Firewall OFF and Firewall ON

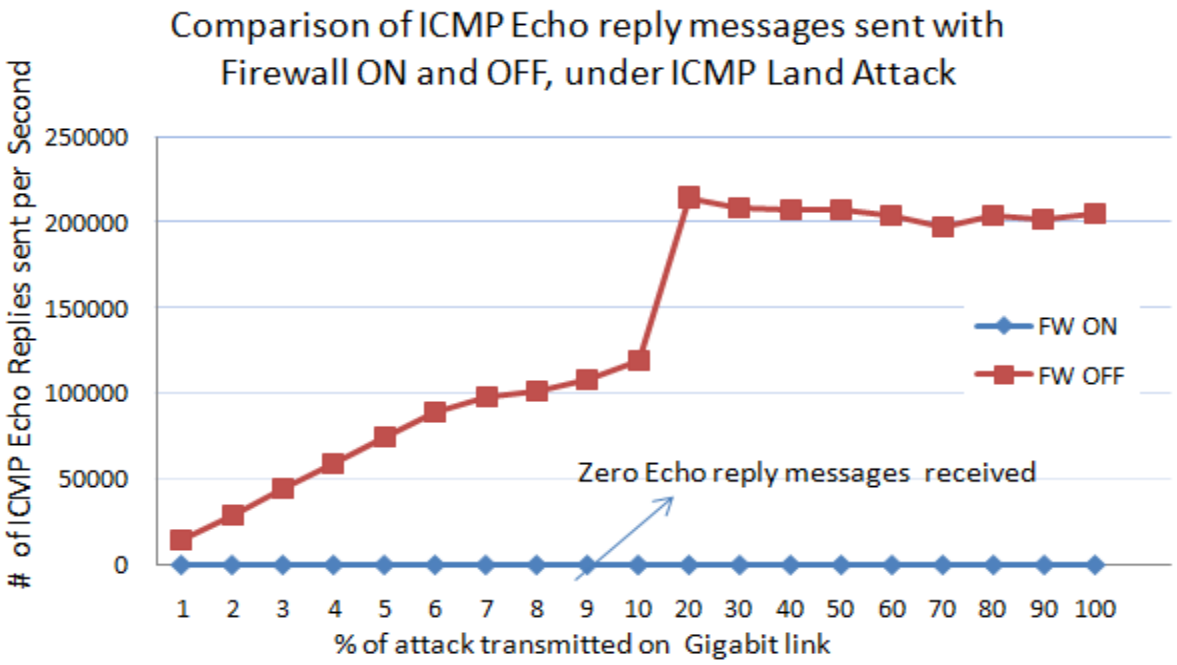
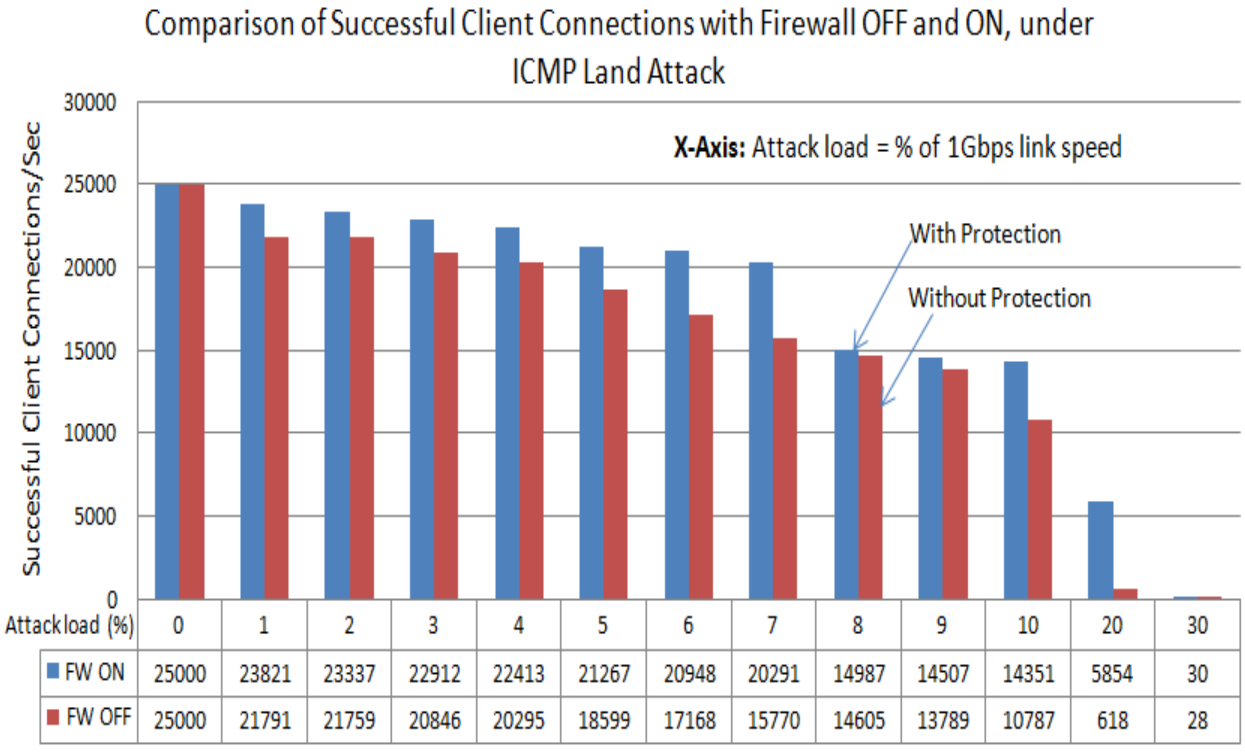



**Figure 2.36:** ICMP-Echo replies sent at the time of ICMP Land Attack on Windows Server 2008 with Firewall OFF compared with Firewall ON

In the Internet, when the legitimate users are receiving service from the server, and at the time if the ICMP Ping-Flood attack is launched on the server, then how is this attack influence the legitimate users, which resembles the situation of real time environment with a busy server, can be observed from figures 2.36 and figure 2.37, where HTTP legitimate traffic with 25,000 Client connections/Sec is maintained towards the server, which is simulated as the traffic coming from different users (Different IP address) all-around the Internet, and the attack traffic of different loads in a range of 10Mbps to 1Gbps is directed towards the server serving the legitimate traffic. The comparison of successful Client connections formed between the server and the legitimate users at the time of attack, at varying loads and with two cases firewall protection enabled and disabled are observed. (Fig. 2.37)




| Attack load (%) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 20 | 30 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FW ON | 25000 | 23821 | 23337 | 22912 | 22413 | 21267 | 20948 | 20291 | 14987 | 14507 | 14351 | 5854 | 30 |
| FW OFF | 25000 | 21791 | 21759 | 20846 | 20295 | 18599 | 17168 | 15770 | 14605 | 13789 | 10787 | 618 | 28 |

**Figure 2.37:** Successful client connections/Second formed at the time of ICMP-Land Attack on Windows Server 2008 with Firewall OFF compared with Firewall ON

From Fig. 2.37, it is observed that the successful legitimate connection are formed with the server by legitimate users are 25,000 per second with no attack traffic. However this number decreases with the increasing of the ICMP-Flood attack load and resulting in almost 600 client connections at 20% (200Mbps) of the attack load with no protection enabled on the firewall. When the server is protected with the protection on the firewall blocking all the illegitimate connections leads to good improvement in the successful connections compared to the case with no protection, however the successful connections are brought down to less than 100 connections at 30% (300Mbps) of attack load. The total number of connections are 10,787 in case with no protection and with protection it is 14,507 at 10% (100Mbps) attack load and at 20% (200Mbps) attack load successful connections are brought down to 618 with no protection, which are more lesser to the case when protection is enabled which recorded as 5,854 connections per second.

From these two cases we observe that Windows server 2008 is defending better with protection enabled on the firewall, when compare with the case, when the protection is disabled, by allowing all the incoming connections, at the time of ICMP Land attack, however at higher loads of attack traffic, even with the protection enabled on the Firewall, blocking all the illegitimate traffic is not able to withstand the attack traffic and is not able to serve the legitimate users, resulting in almost less than 100 successful connections at 300Mbps attack load.

## 2.5 Chapter Summary

From the above results, it was observed that the maximum number of stable client connections formed with the Microsoft Windows server 2003 were 20,000 connections per second and with Windows server 2008 were 25,000 connections per second. These two servers when acting as Web servers were stressed with different DDoS attacks and the impact was studied. Windows server 2003 resulted in 100% processor consumption at 6 Mbps of TCP-SYN attack load. This left with no resources available for the legitimate clients who were trying to get services from the Web server installed on 2003 server. However with Windows server 2008, it was observed that the memory resources were exhausted in no time after the start of TCP-SYN attack resulting in system crash. This resulted in zero client connections at 6 Mbps of SYN attack load. In these cases the servers are protected with default security towards the SYN attack on the operating system itself by Microsoft.

With other DoS attacks such as ICMP-Ping flood, ICMP-Land and UDP Flood attacks both Windows 2003 and 2008 servers resulted in zero legitimate users at higher attack loads on 1Gb link rate. There is an improvement in the number of successful connections at the time of DDoS attacks with the protection, which blocks all the illegitimate connections towards the server and unused ports. But the improvement provided by the firewall was not satisfactory which leads to rapid decrease in the total number of successful connections with the increase in the attack traffic load, and resulted as zero at higher attack loads.

From this chapter, it can be conclude that maximum number of client connections can be formed with windows server 2008 when compared with the windows 2003 under normal

conditions with no attack traffic. But, when the DDoS attacks were sent towards the server Windows Server 2003 had better performance compared with Windows 2008.

# CHAPTER III

## SECURITY PROVIDED BY NETSCREEN 5GT FIREWALL/IPS AGAINST DOS ATTACKS

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 4$^{th}$, 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. Firewall/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 firewalls 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 firewalls/IPS may not always be effective in stopping harmful effects of DoS attacks. It is important to evaluate the capability of Firewall/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 firewall/IPS Juniper Network's Netscreen 5GT[63], to measure its effectiveness in stopping DoS attacks of layer-4 and layer-3, such as TCP-SYN, UDP-Flood, PING-Flood and Land attacks. This firewall is an integrated IPS system that comes with a feature called SYN proxy protection to protect against TCP-SYN based DDoS attacks and UDP-

flood protection to protect against UDP-Flood attack. Performance of the firewall/IPS is measured under protection and compared with its performance when the protection feature was not available (i.e. disabled). It was found that the Juniper's Firewall/IPS was unable to provide satisfactory protection despite the availability of the protection feature against DoS attacks. It is important for the network managers to measure the actual capabilities of an IPS system before its deployment to protect a critical information infrastructure.

### 3.1 Background

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 their media for transferring valuable information, are worrying about securing their systems or networks from attacks on Internet. On August 6$^{th}$ 2009, servers like Twitter, Facebook, Live journal, Google's Blogger and Youtube were under DoS attack, where Twitter was down for several hours [3]. According to "2008 CSI Computer and Security Survey", Firewall type of security technology was used by 94% of the organizations to secure their networks [64, 66]. 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 4$^{th}$, 2009 launched against US and South Korean government websites [1] have caused significant interruption in their operation and now it is prompting many to question the performance of firewalls in defending against such DoS attacks.

Juniper-Networks promotes that the network-based Firewalls recognize and defend known and unknown threats over Internet. Juniper Networks Netscreen 5GT Firewall protects the private networks against attacks like directed attacks, worms, spyware, Trojans, malware and other emerging attacks [67, 68]. With the help of these best capabilities, Netscreen firewall defends the outbreaks at the network level, before they reach the end systems. Internet is having 90% of the traffic as TCP and UDP. So, in this paper, we are motivated to evaluate performance of Juniper networks-Netscreen 5GT firewall and its effectiveness in defending against common Denial of Service attacks in reaching the end systems the communication by consuming the recourses on the legitimate user's network.

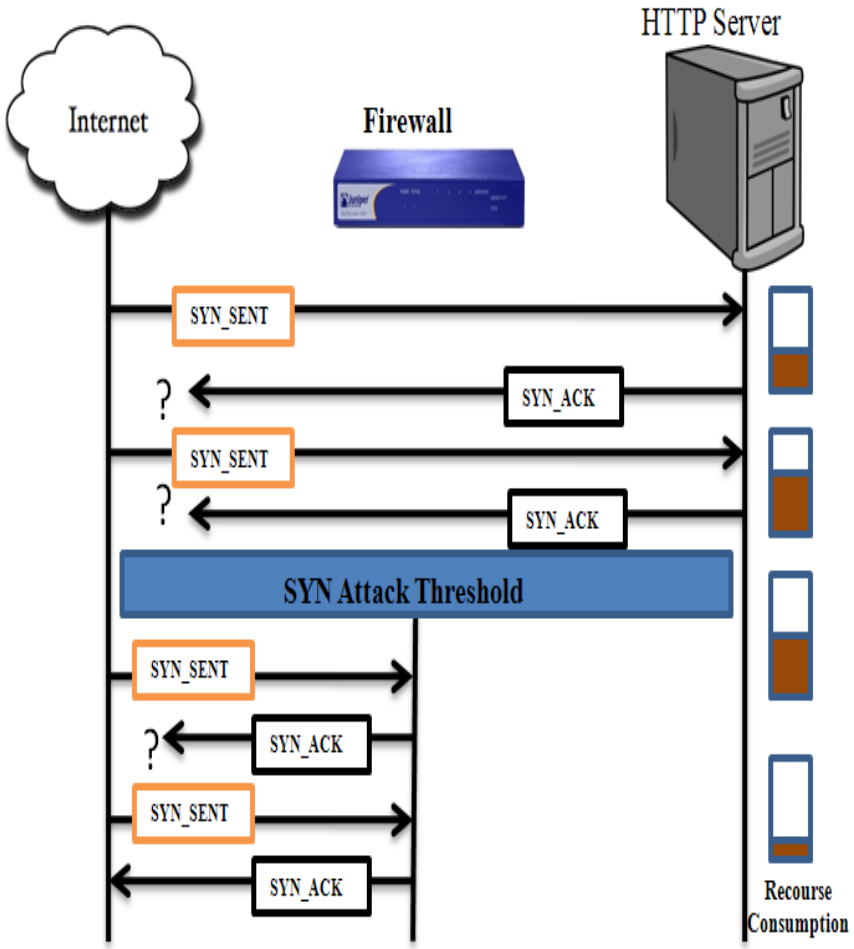



**Figure 3.1:** SYN Proxy protection in Netscreen 5GT [69]

## 3.2 Protection features in Netscreen 5gt Firewall/IPS under DoS attacks

### 3.2.1 TCP-SYN Proxy protection

As Layer-4 TCP-SYN attack is common over Internet due to more than 80% of the total traffic is TCP traffic. And in these TCP attacks, to maintain the reliable connection depends on the various policies of the protocol, which makes the TCP based attacks more common in Internet. And the main reason for the layer-4 TCP-SYN attack is allocating the recourses before completion of full connection, but just after receiving the SYN packets [31-34].

Juniper Networks security devices can impose a limit on the number of SYN segments permitted to pass through the firewall per second. You can base the attack threshold on the destination address and port, the destination address only, or the source address only. When the number of SYN segments per second exceeds one of these thresholds, the security device starts proxying incoming SYN segments, replying with SYN/ACK segments and storing the incomplete connection requests in a connection queue. The incomplete connection requests remain in the queue until the connection is completed or the request times out [69]. In Figure 3.1, the SYN attack threshold has been passed, and the device has started proxying SYN segments.

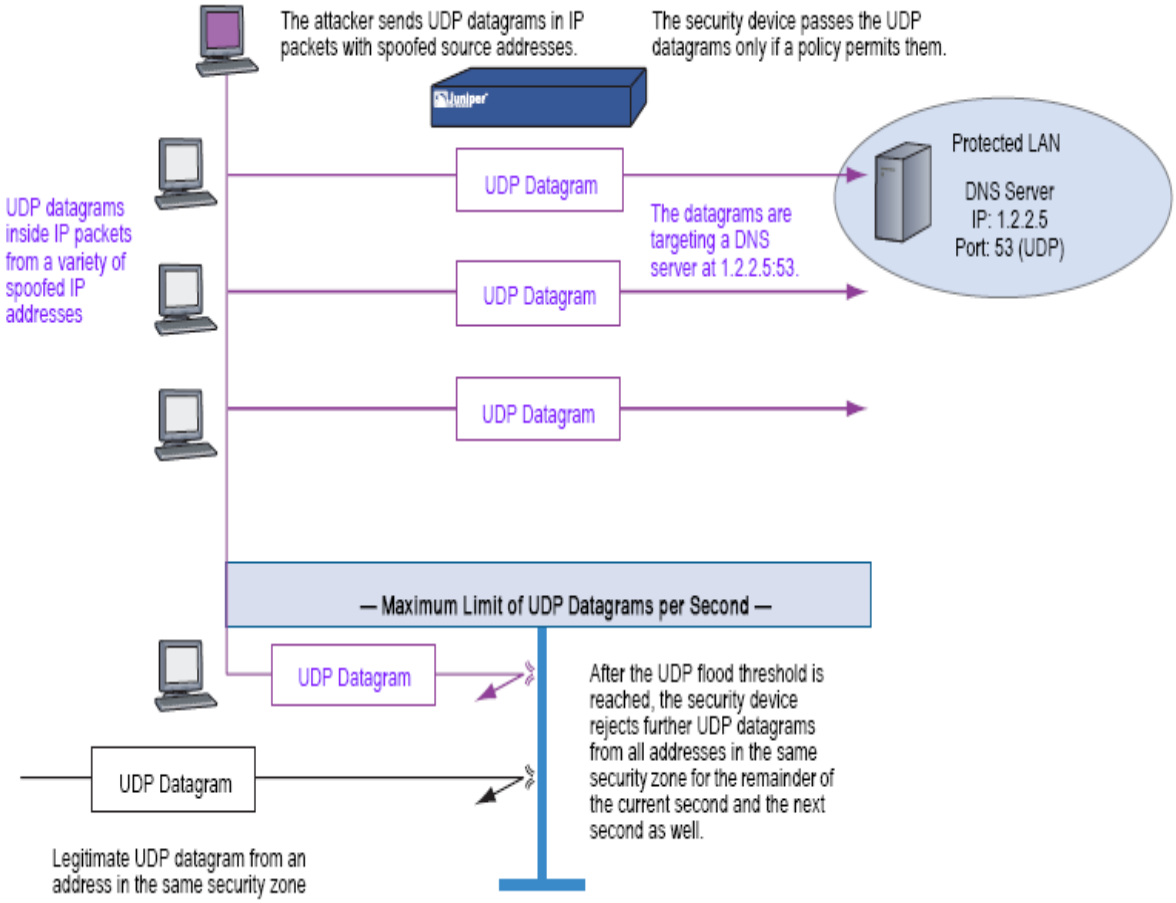



**Figure 3.2:** UDP protection in Netscreen 5GT [69]

### 3.2.2 UDP Flood Protection

As UDP traffic plays a very important role in the Internet, many attackers targets UDP based attacks, which have a capability to bring the whole internet down. This can be happen by attacking the Root DNS servers, which are mainly based on UDP traffic. UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the victim to the point that it can no longer handle valid connections [47-49].

Juniper Networks Netscreen Firewall have a feature of UDP flood protection, which helps in defending the UDP-flood based attacks. After enabling the UDP flood protection feature, you can set a threshold that, once exceeded, invokes the UDP flood attack protection feature. [69] (The default threshold value is 1000 packets per second.) 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 to that destination for the remainder of that second plus the next second as well (Figure 3.2).

### 3.2.3 ICMP Ping attack Protection

Netscreen 5GT has inbuilt protection features to protect against the Layer-3 attacks namely, Ping Flood and ICMP Land Attacks. An ICMP flood typically occurs when ICMP echo requests overload its victim with so many requests that it expends all its resources responding until it can no longer process valid network traffic [40-44]. When enabling the ICMP flood protection feature in Netscreen 5GT, one can set a threshold that once exceeded invokes the ICMP flood attack protection feature [69]. (The default threshold value is 1000 packets per second). If the threshold is exceeded, the Netscreen 5GT firewall ignores further ICMP echo requests for the remainder of that second plus the next second as well. This is well explained in the Figure 3.3.

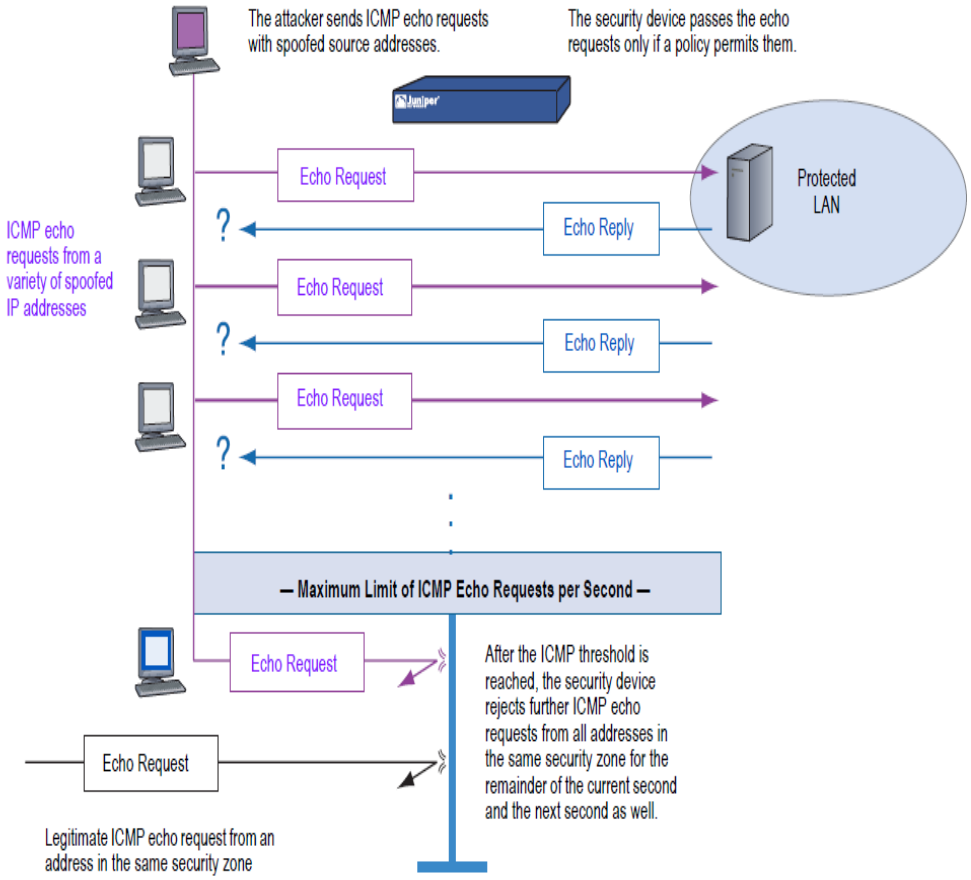



**Figure 3.3:** ICMP Ping Attack protection feature in Netscreen 5GT firewall [69].

### 3.2.4 ICMP Land attack Protection

Combining a SYN attack with IP spoofing, a land attack occurs when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address. The receiving system responds by sending the SYN-ACK packet to itself, creating an empty connection that lasts until the idle timeout value is reached. [45] Flooding a system with such empty connections can overwhelm the system, causing a denial of service. When the SCREEN option to block land attacks is enabled, the security device combines elements of the SYN flood defense and IP spoofing protection to detect and block any attempts of this nature. [69]

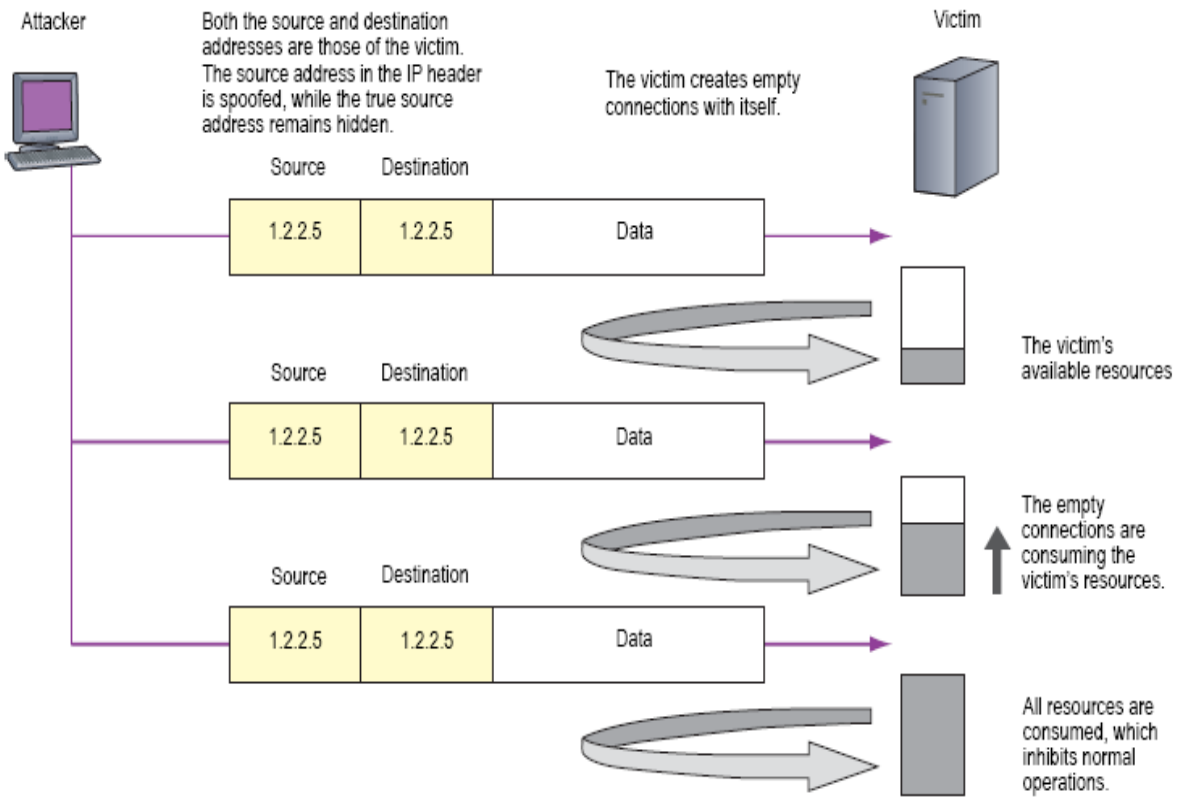



**Figure 3.4:** ICMP Land Attack protection feature in Netscreen 5GT firewall [69].

### 3.3 Experimental setup

In the controlled lab environment, we developed a secured network environment as shown in Figure 3.4, where we launched a TCP-SYN attack to observe the performance of Netscreen 5GT firewall. For this experiment the Juniper Networks-Netscreen 5GT Firewall and Windows Server 2003 on Intel® Xeon™ 3GHz, 3GHz Processor with 4GB RAM are considered. The maximum numbers of TCP connections per second that the server can form were 20,000 connections.

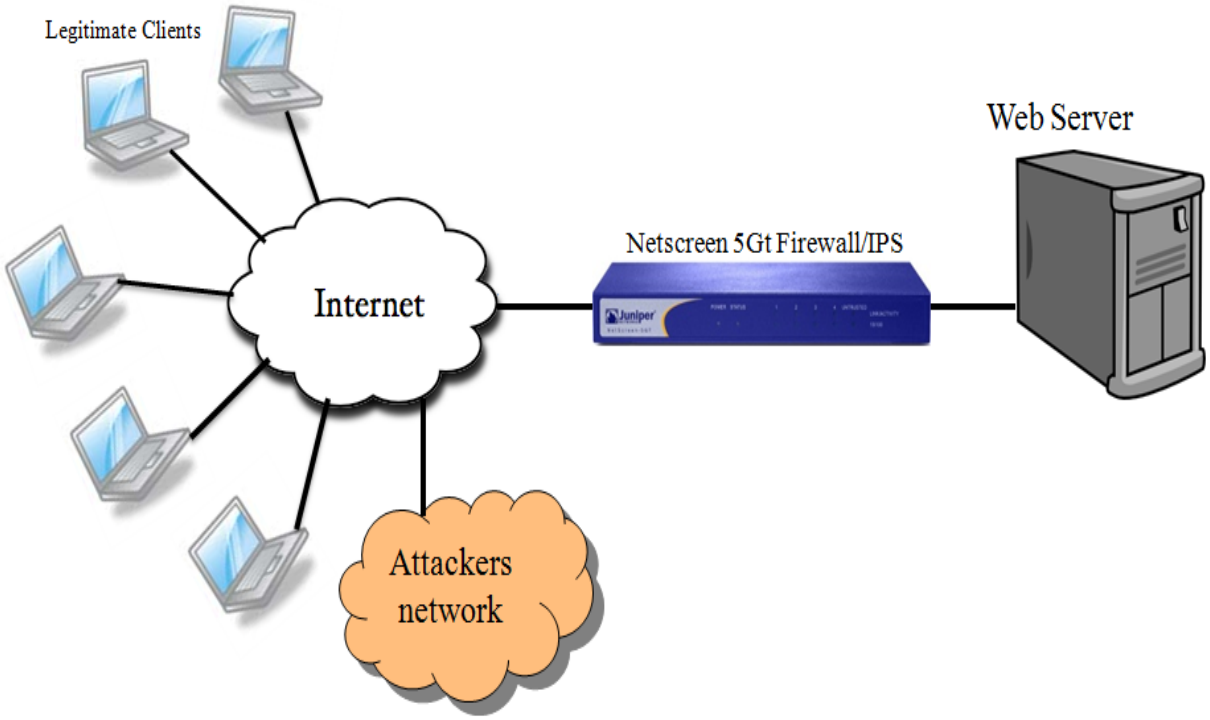



**Figure 3.5:** Experimental setup to find the maximum number of stable connections formed by the server through firewall.

## 3.4 Results and Discussion

### 3.4.1 Maximum number of stable client connections per second, formed by the server through Netscreen 5GT

The Netscreen 5GT firewall is placed between the Web-Server and the Internet as shown in figure 3.5. The TCP legitimate client traffic is simulated, in the controlled lab environment as it is initiated from different IP address and port numbers that resembles the original or real-time environment in Internet. Using this traffic continuous TCP connections are maintain between the Server and Clients.

The maximum number of successful client TCP connections per second are 600. In this case, no attack traffic (illegitimate traffic) was sent towards the server and also there is no protection (allowing all type of connections) configured on the Netscreen 5GT firewall. So, this 600 connections per second is the number that states the maximum capability of the firewall depending on the resources (Processor, Memory and Bandwidth), which are stable.

### 3.4.2 Performance of Netscreen 5GT firewall/IPS under TCP-SYN attack

**3.4.2.1 TCP SYN Attack on server without any protection on Firewall/IPS.** In this case the firewall was setup with no protection and server was maintained with continuous 600 TCP connections per second all over the experiment. The TCP- SYN attack load varying from 1Mbps to 100Mbps insteps of 10Mbps is sent towards the server, through the firewall and observed the number of successful TCP-connections per second that are formed by the server at different loads of TCP-SYN flood attack are observed. The experimental setup can be seen in figure 3.5, where the legitimate HTTP clients are trying to connect to the server from Internet and at the same time the attacker from the Internet direct TCP-SYN attack in varying loads from 1Mbps to 100Mbps towards the server.

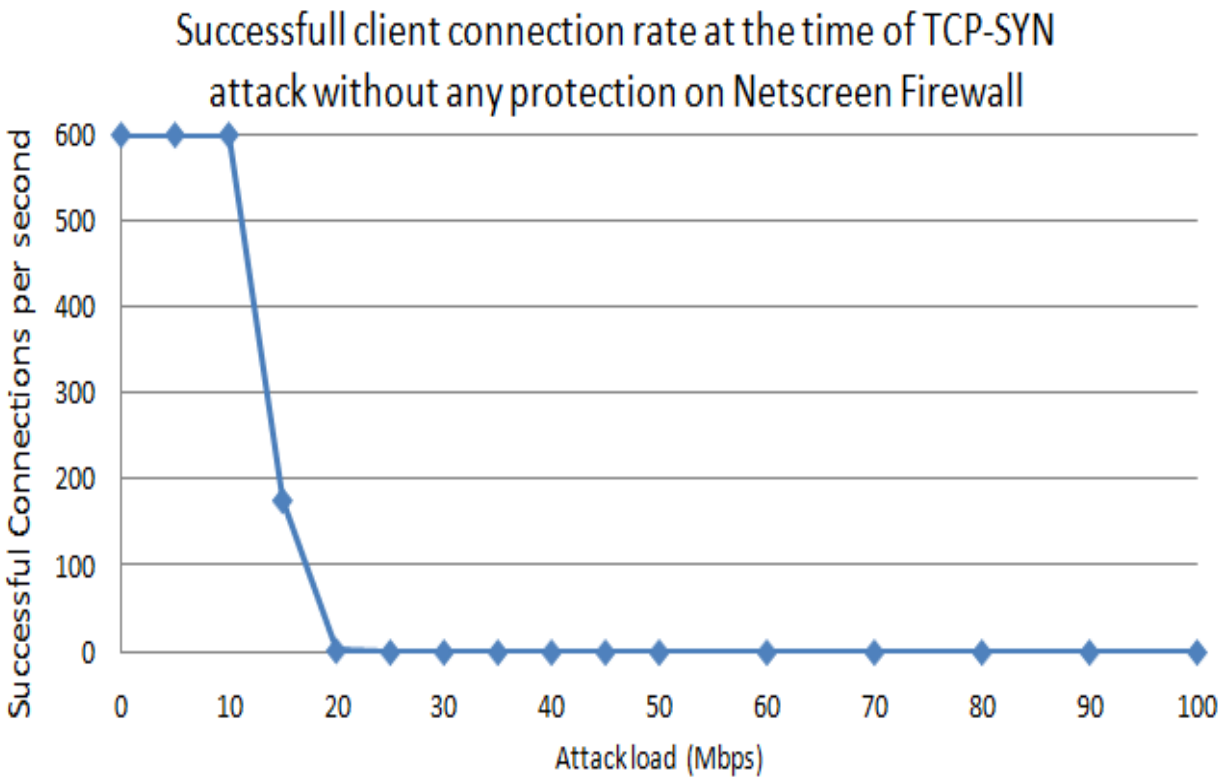



**Figure 3.6:** Connections per second at different SYN attack loads with no protection on firewall.

From this experiment, we found that the legitimate connections are brought down to zero at the TCP-SYN attack load of 20Mbps (Figure 3.6). So the attacker has succeeded in preventing the legitimate users from obtaining the services at 20 Mbps of attack traffic load. When the SYN attack load is zero, the number of successful connections are 600, and when the attack load increases to the point of 20Mbps, it can be seen that the number of successful connections dropped to zero rapidly. This is possibly due to lack of resources which may be consumed by the attack traffic that left no resources for the legitimate users.

**3.4.2.2 TCP SYN attack on server with SYN-Proxy protection enabled on firewall/IPS.** In this case the firewall was setup with SYN- protection and server was maintained with continuous 600 TCP connections per second all over the experiment. The threshold values are set as the default values (200 half open connections per second) given by Netscreen 5GT firewall. The TCP- SYN attack load varying from 1Mbps to 100Mbps insteps of 10Mbps was sent to the server, through the firewall and the number of successful TCP-connections per second are formed by the server at different loads of TCP-SYN flood attack are observed. The experimental setup with Syn-protection on the firewall can be seen in figure 3.5. Where the TCP-SYN packets received by the firewall after crossing threshold value of the half-open connections, the firewall itself acts as the proxy between the server and the Internet. This allows the connections to be formed between the server and the clients from the Internet only after making sure that the connection is legitimate.

When the SYN-Proxy protection was enabled on the firewall, it was found that the successful connections rate changes from 600 Connections per second at zero attack load, to zero connections per second at 50Mbps attack load. This rapid decrease in successful connection rate, varying with the attack load, results in no legitimate user utilizing the services from server at 50Mbps of attack traffic load and can be seen in figure 3.7.

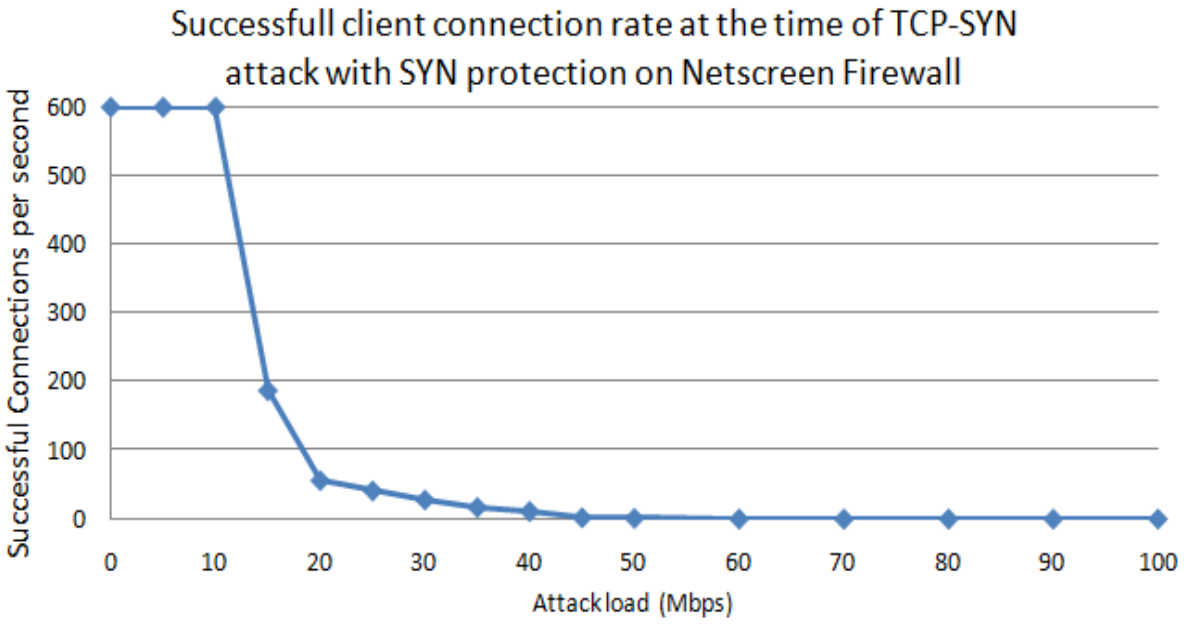



**Figure 3.7:** Connections per second at different SYN attack load with SYN Proxy protection on firewall

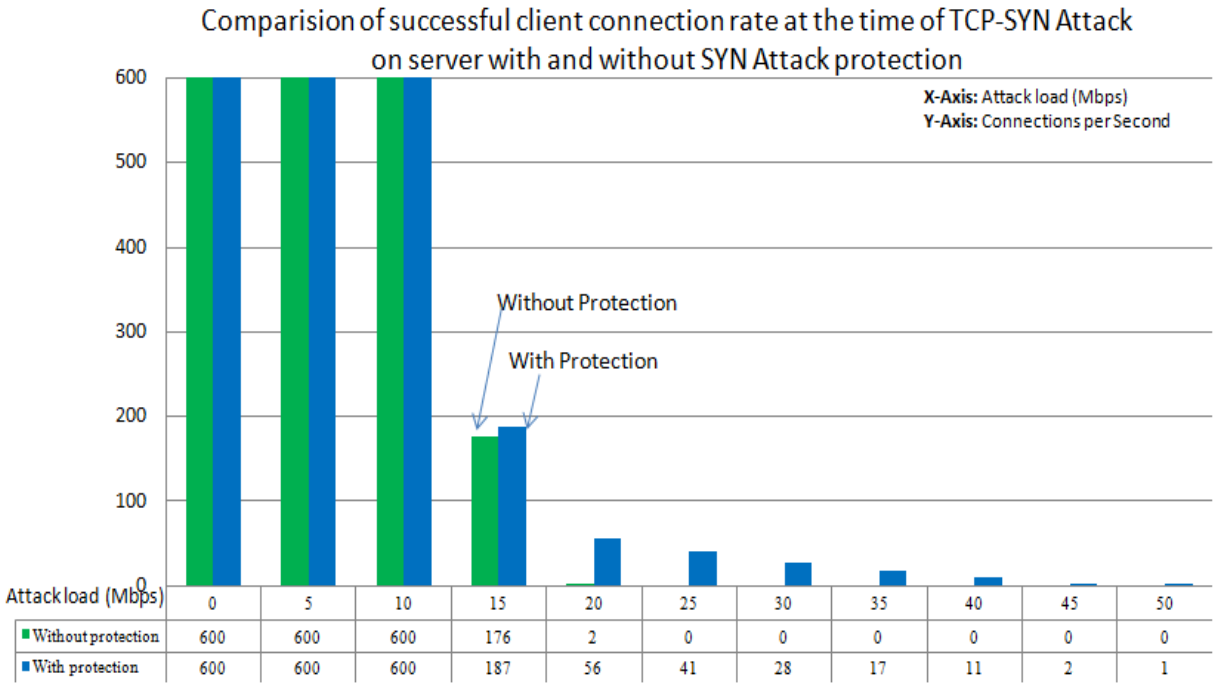



**Figure 3.8:** Comparison of successful client connections at the time of TCP-SYN attack at different attack load with and without SYN-Proxy attack protection on Netscreen 5GT Firewall

**3.4.2.3 Comparison of Successful connections per second with and without SYN protection on Netscreen 5GT firewall/IPS.** Figure 3.8 shows the connections formed per second for the both scenarios with SYN-Proxy protection and without SYN-Proxy protection enabled. It was observed that without Syn-proxy protection, the successful connection rate was zero after 18Mbps of TCP-SYN attack traffic load. In the case with SYN-Proxy protection enabled on the firewall, the successful connection rate was zero after 40Mbps of attack traffic load. From these experiments one can understand that the Netscreen 5GT firewall was able to sustain the TCP-SYN flood attack traffic only up to 40Mbps of attack traffic load and there after the connection rate was found to be zero with the SYN-Proxy protection. This improvement in performance, as compared with the zero connection rates at 18Mbps of attack traffic load without SYN-Proxy protection is of not much use as the availability of the server to its hosts is zero at such attack traffic load of 40Mbps. This shows that the performance improvisation provided by Juniper networks-Netscreen 5GT Firewall is not satisfactory as one would expect to get the protection throughout the attack period with the SYN-Proxy protection.

### 3.4.3 Performance of Netscreen 5GT firewall/IPS under UDP Flood attack

#### 3.4.3.1 UDP Flood Attack on server without any protection enabled on Firewall/IPS.

In this case the firewall was setup with no protection and server was maintained with continuous 600 TCP connections per second all over the experiment. The UDP flood attack traffic load varying from 1Mbps to 100Mbps in steps of 10Mbps is sent towards the server through the firewall. The number of successful TCP-connections per second that are formed by the server at different loads of UDP flood attack are observed and plotted.

When the server is flooded with the UDP flood traffic, which pass through the stateful firewall, will possibly leads the firewall to consume all of its resources. This is due to

maintaining the sessions for every packet that are passing through. UDP packets received by the server process the packets and checks for the application on the requested port number. If there is no application on that requested port, server sends the destination unreachable packet as reply for the received packets. To maintain sessions for all of the packets passing through the firewall causes over head on the firewall that may possibly consumes all of its critical resources in processing and maintaining the sessions for the attack traffic which lead to limited resources on the firewall for the legitimate users.

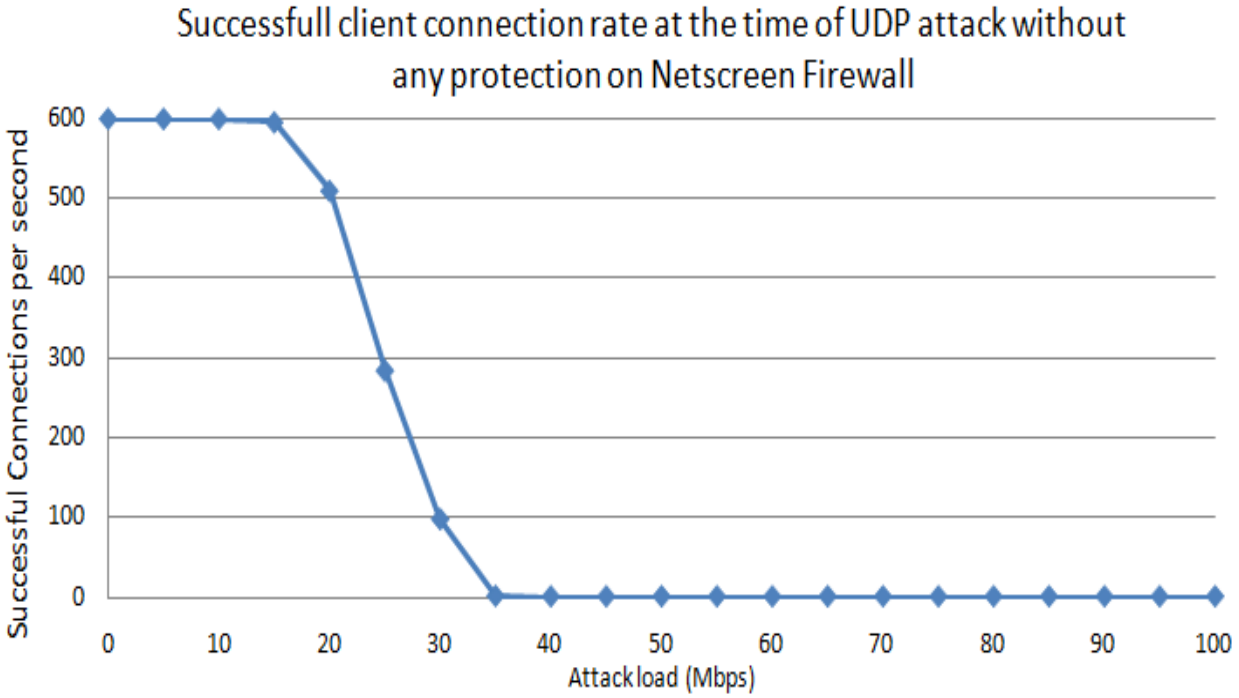



**Figure 3.9:** Successful connections per second at different UDP Flood attack loads with no protection on firewall

From this experiment, it is found that the number of successful connections were dropped to zero rapidly from 35Mbps of attack traffic load (Figure 3.9). This is possibly due to the consumption of resources by the illegitimate traffic.

**3.4.3.2 UDP flood attack on server with UDP Flood protection enabled on firewall/IPS.** In this case the firewall was setup with UDP Flood attack protection enabled with default threshold limit of 1000 Packets per second and server was maintained with continuous 600 TCP connections per second all over the experiment. The UDP flood attack load varying from 1Mbps to 100Mbps in steps of 10Mbps is sent towards the server, through the firewall.

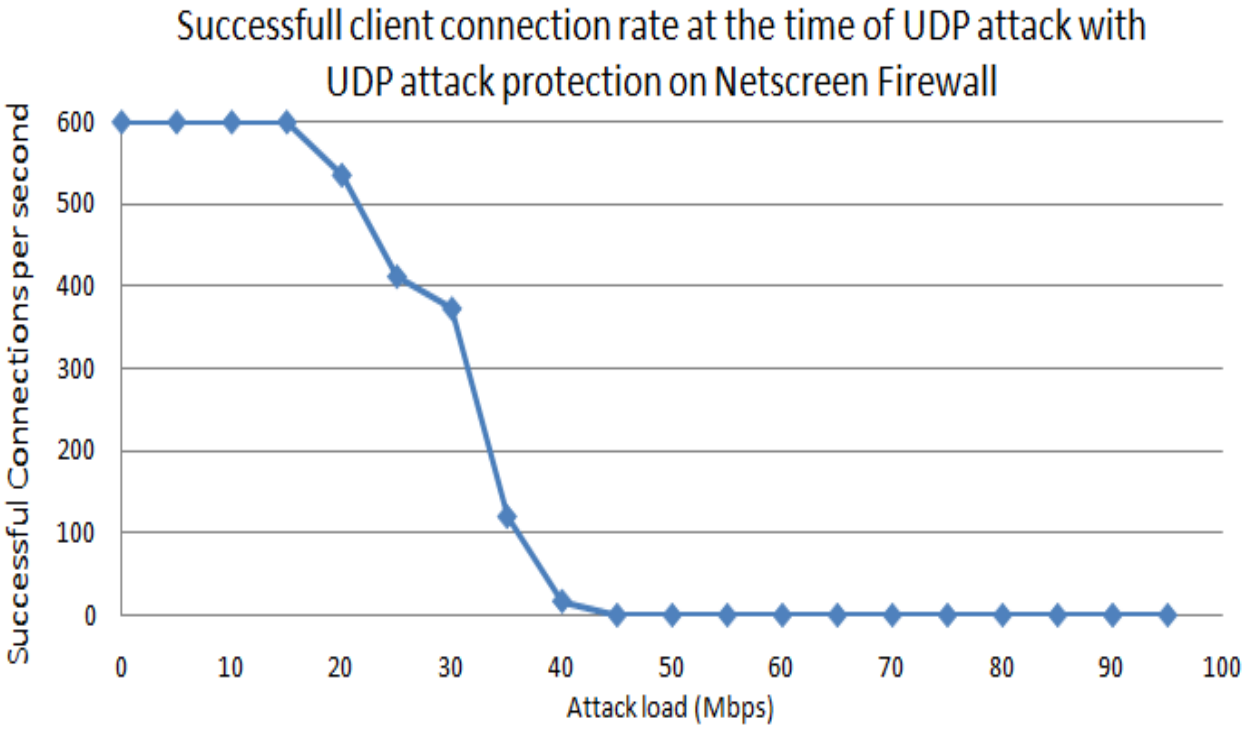
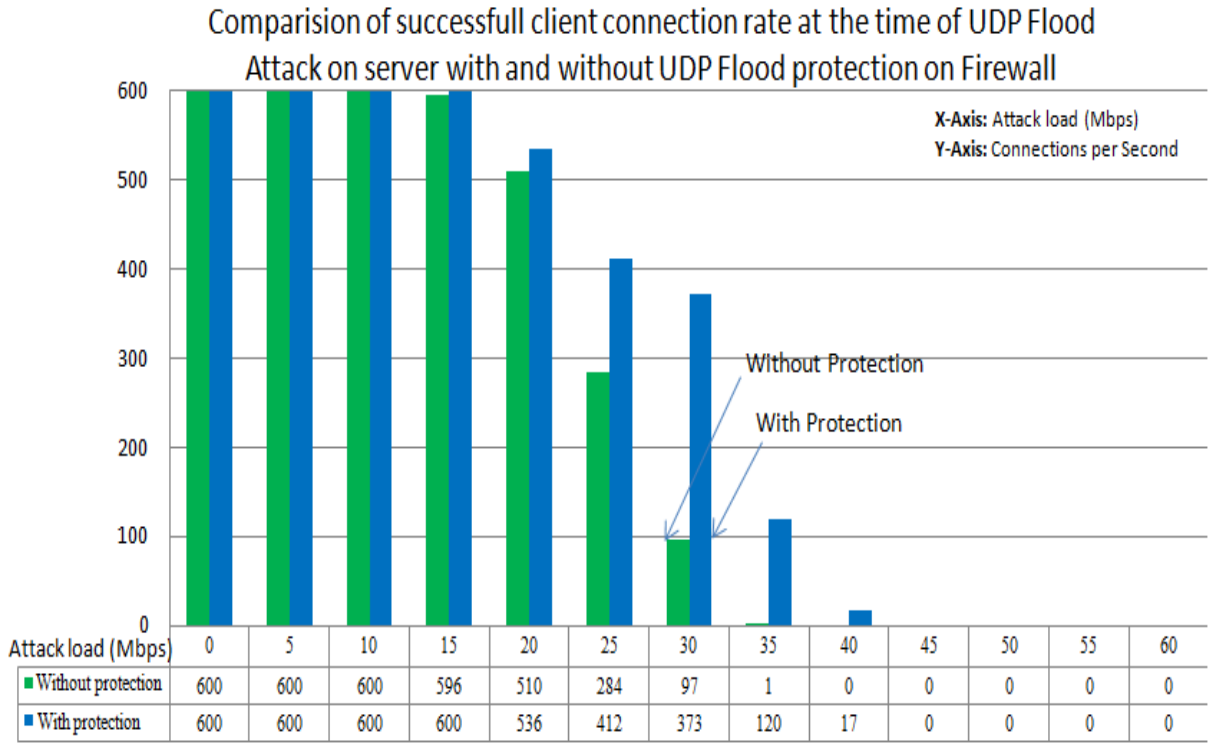



**Figure 3.10:** Successful connections per second at different UDP-Flood attack loads with Land attack protection enabled on the firewall

When the UDP flood protection was enabled on the Juniper Networks-Netscreen 5GT firewall, it is found that the successful connections rate changes from 600 Connections per second at no attack load, to zero connections per second at 45 Mbps of attack load. Even with the protection available on the firewall, the connection rate was not stable and was dropped to zero at 45Mbps UDP-Flood attack load (Figure 3.10). This may be possibly due to, the resource consumption by the attack traffic in detecting and dropping the UDP-Flood packets.




| 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 3.11:** Comparison of successful client connections at the time of UDP-Flood attack at different attack loads with and without UDP-Flood attack protection on Netscreen Firewall

**3.4.3.3 Comparison of Successful connections per second with and without UDP Flood Protection on Netscreen 5GT firewall/IPS under UDP Flood attack.** From figure 3.11, it was observed that without UDP Flood-protection, the successful connection rate was zero at 35Mbps of UDP-Flood attack traffic load, and with the UDP-Flood attack protection enabled on the firewall; the connection rate was zero at 45Mbps attack traffic load. The successful connections without protection are 284 and with protection are 412 at 25Mbps attack load, and at 35Mbps attack load without protection on firewall the total connections are zero and with protection they are 120 successful connections. By observing these results, it is found that the protection on the firewall increases the successful number of connection at lower attack load, but

at higher attack load which is after 45Mbps attack load, protection on the firewall was not able to defend the UDP-Flood attack.

### 3.4.4 Performance of Netscreen 5GT firewall/IPS against ICMP Ping attack.

**3.4.4.1 ICMP Ping Flood Attack on server without any protection enabled on Firewall/IPS.** In this case the firewall is setup with no protection and server is maintained with continuous 600 TCP connections per second all over the experiment. The ICMP-Ping attack load varying from 1Mbps to 100Mbps in steps of 10Mbps is sent towards the server through the firewall and the number of successful TCP-connections per second that are formed by the server at different loads of ICMP-Ping flood attack are observed and plotted.

When the server was flooded with the ICMP-Ping requests which are passing through the firewall that maintains all the sessions for each and every packet that are passing through will leads to the firewall consuming all of its resources. The consumption of all of its critical resources of the firewall in processing the packets and maintaining the sessions for the attack traffic, leads to limited resources on the firewall for the legitimate users.

From this experiment, we found that the legitimate connections are brought down to zero at the ICMP-ping attack traffic load of 20Mbps. So the attacker was succeeded in avoiding the legitimate users from utilizing their services at 20Mbps of attack traffic load. The graph showing the connections rate versus attack traffic load is shown in figure 3.12. When the ICMP-Ping attack load was zero, the number of successful connections are 600, when the attack load increases to the point of 20Mbps, the number of successful connections are dropped down to zero linearly. This states that the resources are totally consumed by attack traffic load, which intentionally prevented the legitimate users from getting service from the server.

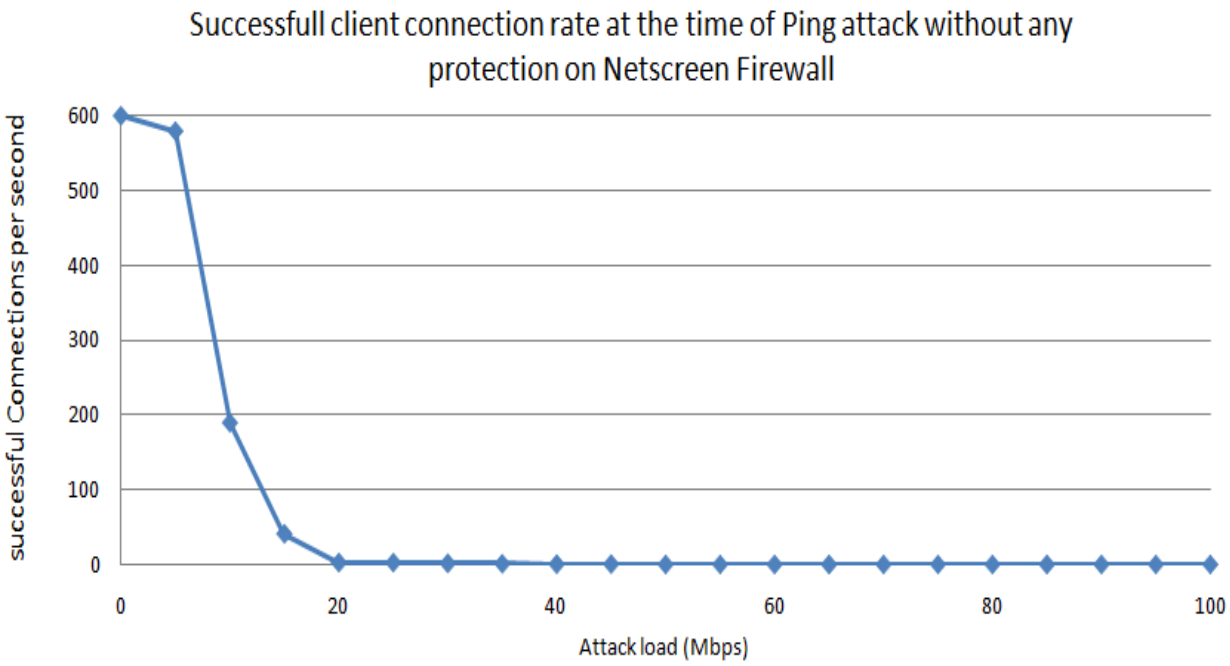



**Figure 3.12:** Successful connections per second at different ICMP-Ping attack loads with no protection on firewall

**3.4.4.2 ICMP-Ping flood attack on server with ICMP protection enabled on firewall/IPS.** By enabling the protection on the firewall by setting a threshold level, the firewall allows the ICMP packets through it till it reaches the threshold and there after drops all further ICMP packets it receives. In real time getting a flood of ICMP packets will not happen often, so getting up a threshold limit depending on the traffic in a network will help legitimate users in getting services without any interrupt.

In this case the firewall was setup with ICMP protection and server was maintained with continuous 600 TCP connections per second all over the experiment. The threshold values are set as the default values given by Netscreen 5GT firewall. The ICMP-Ping attack load varying from 1Mbps to 100Mbps in steps of 10Mbps is sent to the server, through the firewall and the number of successful TCP-connections per second are formed by the server at different loads of ICMP-Ping flood attack are observed.

When the ICMP-Proxy protection was enabled on the firewall, with default threshold value on Juniper Networks-Netscreen 5GT firewall, it was found that the successful connections rate changes from 600 Connections per second at no attack load, to zero connections per second with the Ping attack traffic load increases and reaches to 30Mbps. This linear decrease in successful connection rate varying with the attack load resulting in no legitimate user utilizing the services from server after 30Mbps of attack traffic load can be seen in figure 3.13.

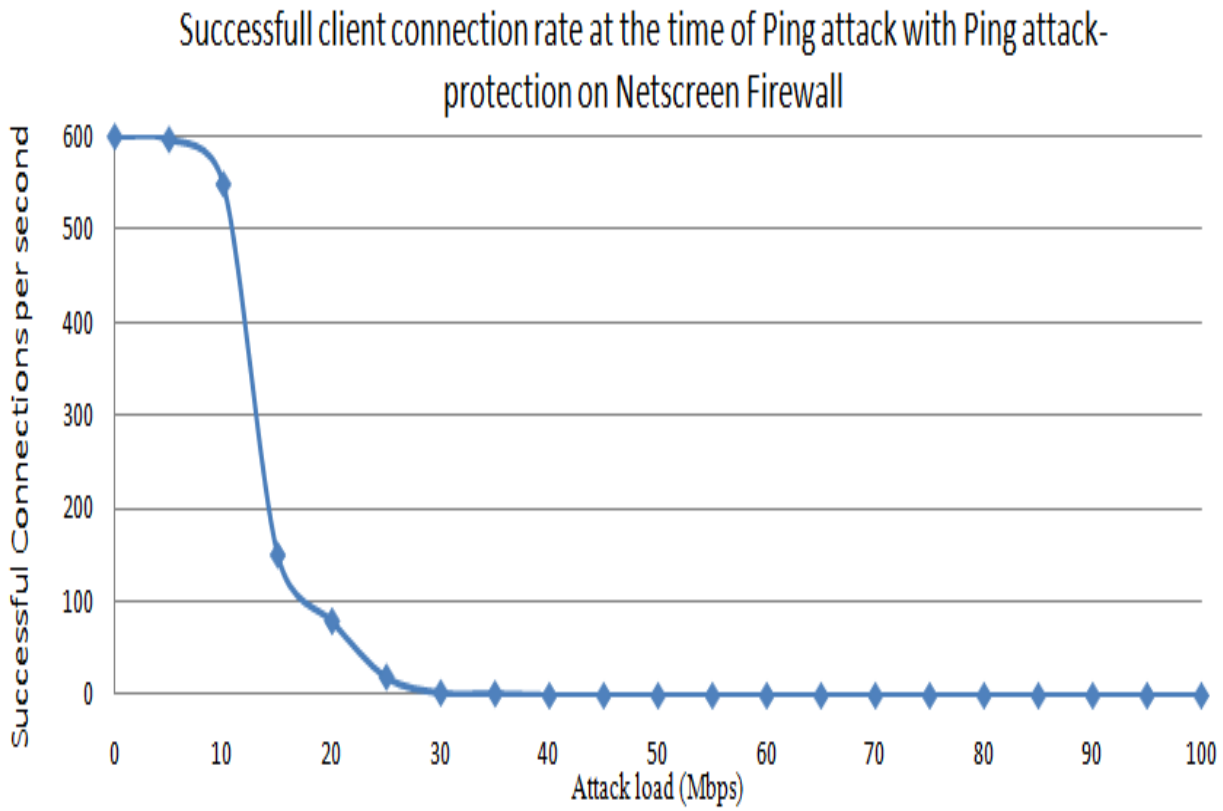
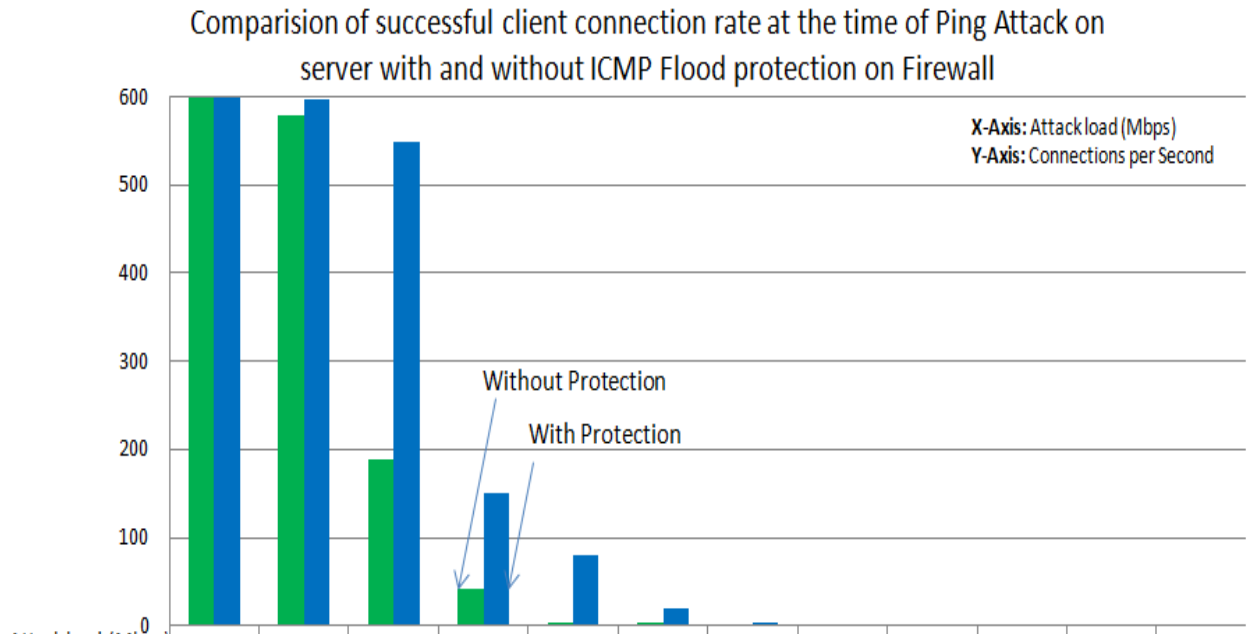



**Figure 3.13:** Successful connections per second at different ICMP Ping attack loads with ICMP Flood attack protection on firewall

### 3.4.4.3 Comparison of Successful connections per second with and without ICMP Flood Protection on Netscreen 5GT firewall/IPS.

From figure 3.14, it is observed that without ICMP-protection, the successful connection rate was zero after 20Mbps of ICMP-Ping attack traffic load. Is in the case of ICMP-Ping protection enabled on the firewall, the successful connection rate was zero after 30Mbps of attack traffic load. From these results one can infer that, the Netscreen 5GT firewall was able to sustain the ICMP-Ping flood attack for traffics only up to 30Mbps and there after the connection rate was found to be zero even with the protection. There is an increase in connection rate compared with the firewall without protection; however the performance improvisation provided by Juniper networks-Netscreen 5GT Firewall is not satisfactory as one would expect to get the protection throughout the attack period with the SYN-Proxy protection.




| Attack load (Mbps) | 0 | 5 | 10 | 15 | 20 | 25 | 30 | 35 | 40 | 45 | 50 | 55 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Without protection | 600 | 580 | 190 | 41 | 3 | 3 | 2 | 1 | 1 | 1 | 0 | 0 |
| With protection | 600 | 597 | 549 | 151 | 80 | 20 | 3 | 2 | 0 | 0 | 0 | 0 |

**Figure 3.14:** Comparison of successful client connection at the time of ICMP-Ping attack at different attack loads with and without ICMP Flood attack protection on Netscreen 5GT Firewall

### 3.4.5 Performance of Netscreen 5GT firewall/IPS under ICMP Land attack.

#### 3.4.5.1 ICMP Land Attack on server without any protection enabled on Firewall/IPS.

In this case, the firewall was setup with no protection and server was maintained with continuous 600 TCP connections per second all over the experiment. The ICMP-Land attack load varying from 1Mbps to 100Mbps in steps of 10Mbps is sent towards the server through the firewall and the number of successful TCP-connections per second that are formed by the server at different loads of Land attack are observed and plotted.

When the server was flooded with the land attack traffic, that passes through the stateful firewall which maintains all the sessions for every packet passing through it will leads to resource consumption on the firewall resources. The consumption of all of its critical resources in processing maintaining the sessions for the attack traffic, leads to no limited resources on the firewall for the legitimate users. As land attack have the same IP address as source and destination IP address on the echo request, the echo reply send by the server will reach to itself.

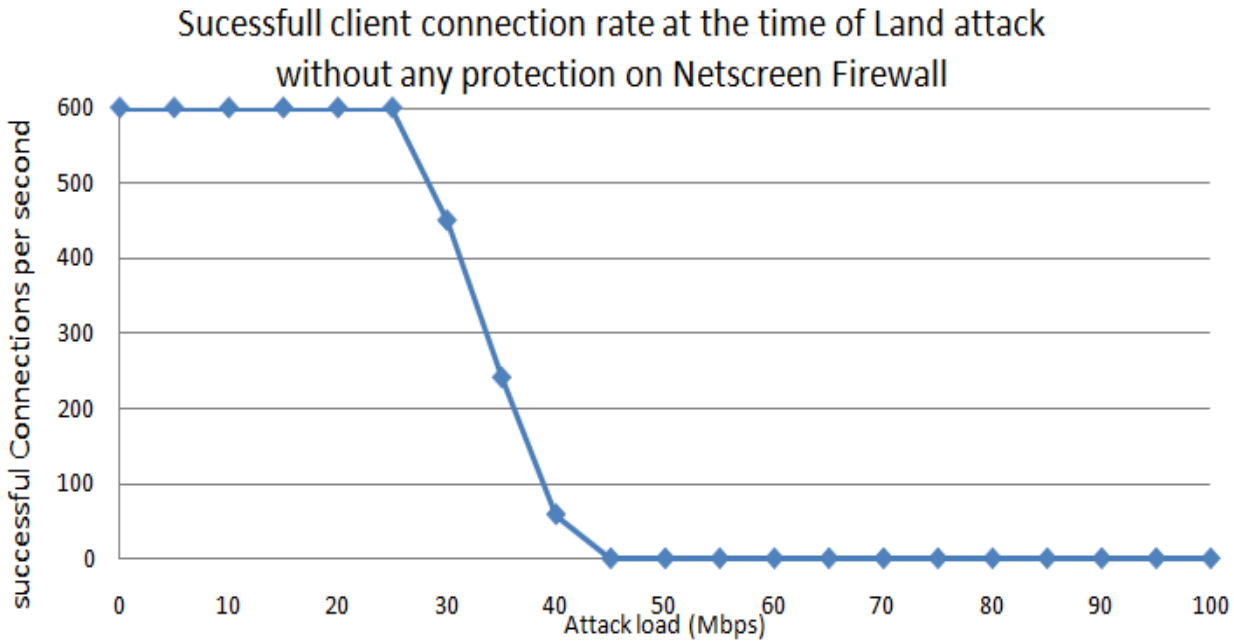



**Figure 3.15:** Successful connections per second at different ICMP Land attack loads with no protection on firewall

From this experiment, it was found that the number of successful connections are linearly dropped to zero at 45Mbps of attack traffic load, which states that the resources are totally consumed by attack traffic load that succeeds in preventing the legitimate users from getting services from the server (Figure 3.15).

**3.4.5.2 ICMP Land attack on server with ICMP protection enabled on firewall/IPS.** ICMP is the protocol used for diagnostic purpose. However in the real time, packet with same source and destination address are no where seen on the Internet. So a packet with same source and destination address can be identified as land attack traffic and can be discarded. The main intention of this kind of traffic is to bring down the system by making it process the illegitimate traffic and also make it to reply itself, so that more resources are consumed in processing all those packets received. By setting the ICMP Land attack protection on the firewall, any ICMP packet which are with same source and destination address are dropped, instead of forwarding them towards the server.

In this case the firewall was setup with ICMP Land attack protection and server was maintained with continuous 600 TCP connections per second all over the experiment. The Land attack load varying from 1Mbps to 100Mbps in steps of 10Mbps is sent to the server, through the firewall.

When the ICMP-Proxy protection is enabled on the Juniper Networks-Netscreen 5GT firewall, it is found that the successful connections rate changes from 600 Connections per second at no attack load to zero connections per second when the Land attack traffic load increases and reaches to 45Mbps of attack traffic load. Even with the protection available on the firewall, the connection rate was not stable and was dropped to zero at 45Mbps of land attack load (Figure 3.16).

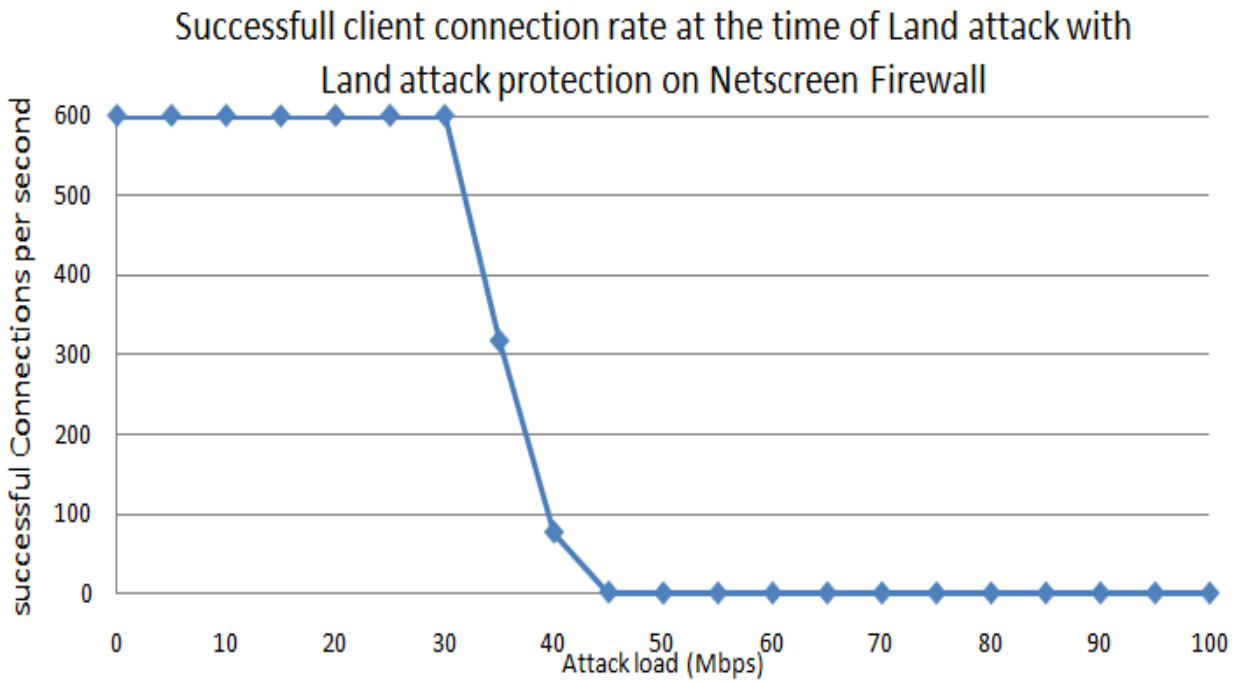
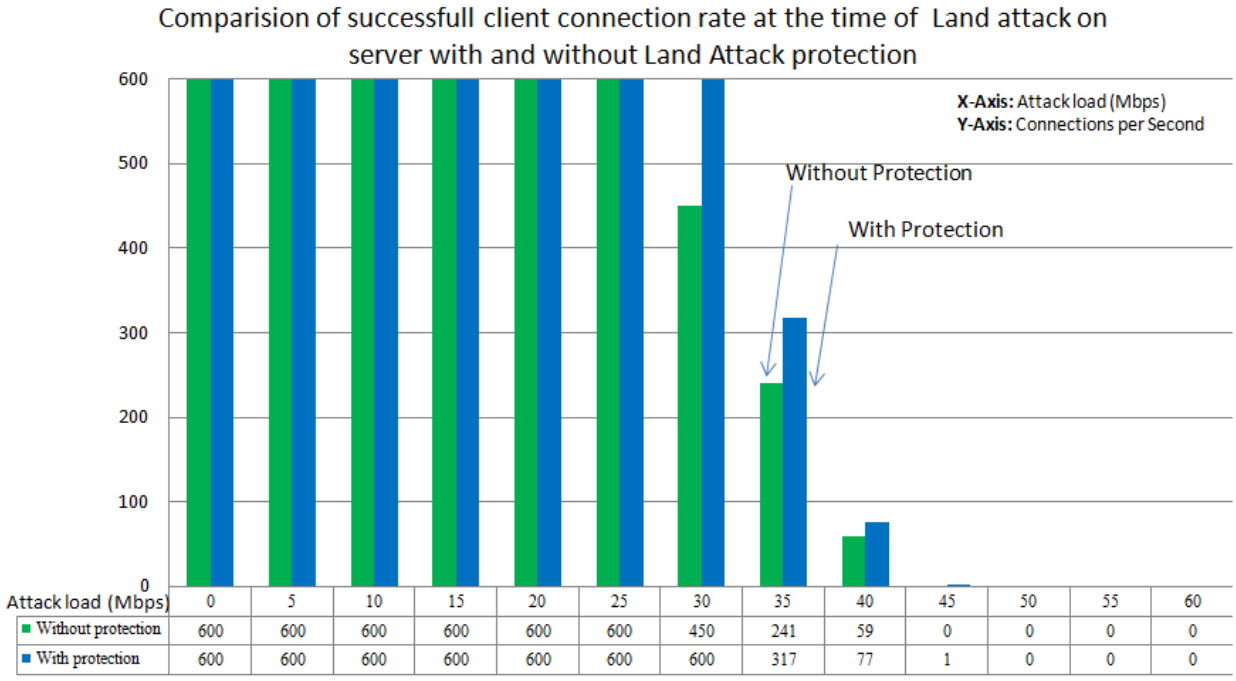



**Figure 3.16:** Successful connections per second at different ICMP Land attack loads with Land attack protection enabled on the firewall




| Attack load (Mbps) | 0 | 5 | 10 | 15 | 20 | 25 | 30 | 35 | 40 | 45 | 50 | 55 | 60 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Without protection | 600 | 600 | 600 | 600 | 600 | 600 | 450 | 241 | 59 | 0 | 0 | 0 | 0 |
| With protection | 600 | 600 | 600 | 600 | 600 | 600 | 600 | 317 | 77 | 1 | 0 | 0 | 0 |

**Figure 3.17:** Comparison of successful client connection at the time of ICMP-Land attack at different attack loads with and without land attack protection on Netscreen Firewall

**3.4.5.3 Comparison of Successful connections per second with and without ICMP Land attack protection on Netscreen 5GT firewall/IPS.** From figure 3.17, it is observed that without ICMP Land attack protection, the successful connection rate is zero at 45Mbps of Land attack traffic load, and also with the land attack protection enabled on the firewall; the connection rate was zero at 45Mbps attack traffic load. There is a difference in number of connections maintained in these two cases. When the firewall is configured to have ICMP Land protection the number of connections formed are more when compare to the case without protection, which was observed from the figure 3.17, at 30mbps attack traffic load the successful are 450 per second without protection, which are improved to 600 connection with protection. At 35Mbps attack traffic load 241 connections are formed without protection, which are improved to 317 connections with protection ICMP-Land protection enabled on the firewall. But in both cases the legitimate users got denied of the service by the server at 45Mbps of Land attack traffic load.

## 3.5 Chapter Summary

In this chapter the performance of Juniper Networks Netscreen 5GT firewall under TCP-SYN flood, UDP-Flood, ICMP-Ping Flood and ICMP-Land attacks type of DDoS attacks was observed. The maximum numbers of stable client connections formed by server through the firewall were 600 connections per second. When the firewall was stressed with TCP-SYN attack traffic, it was able to sustain up to 40Mbps and there after the connection rate was found to be zero with SYN-Proxy protection enabled. Without the SYN-Proxy protection the connection rate was zero at 18Mbps of attack load on 100Mbps Fast Ethernet link.

In case of ICMP-Ping attack, it was observed that the connection rate was zero at 30Mbps of attack load with protection enabled. Without protection the connection rate was zero at 20 Mbps of attack load. In case of ICMP-Land flood attack, the connection rate was found to be

zero at 40Mbps of attack load for both the cases, i.e.; with protection and without protection. The only difference was that the number of connections were more with protection enabled.

With UDP-Flood protection enabled the number of connections were brought down to zero at 45Mbps of attack load and connections were brought to zero at 30Mbps of attack load traffic with no protection. There was an improvement in connection rate when the protection was enabled in all the attacks.

# CHAPTER IV

# EVALUATION OF CISCO ASA 5510 ROUTER/IPS UNDER DENIAL OF SERVICE ATTACKS

In this chapter, we evaluate performance of Cisco ASA-5510 is a router with integrated 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 [70]. In this chapter, we measure the impact of Denial of Service Attack (DoS) on Cisco ASA 5510 Router/IPS, 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 [71-77]. Despite of security systems installed, servers have been compromised due to DoS attacks [78-79]. The availability and security provided by the Cisco ASA Router/IPS when it is defending against the DoS attacks explains the performance of the ASA.

## 4.1 Protection features in Cisco ASA Router/Intrusion prevention system towards the Denial of Service attacks

### 4.1.1 TCP-SYN Proxy protection

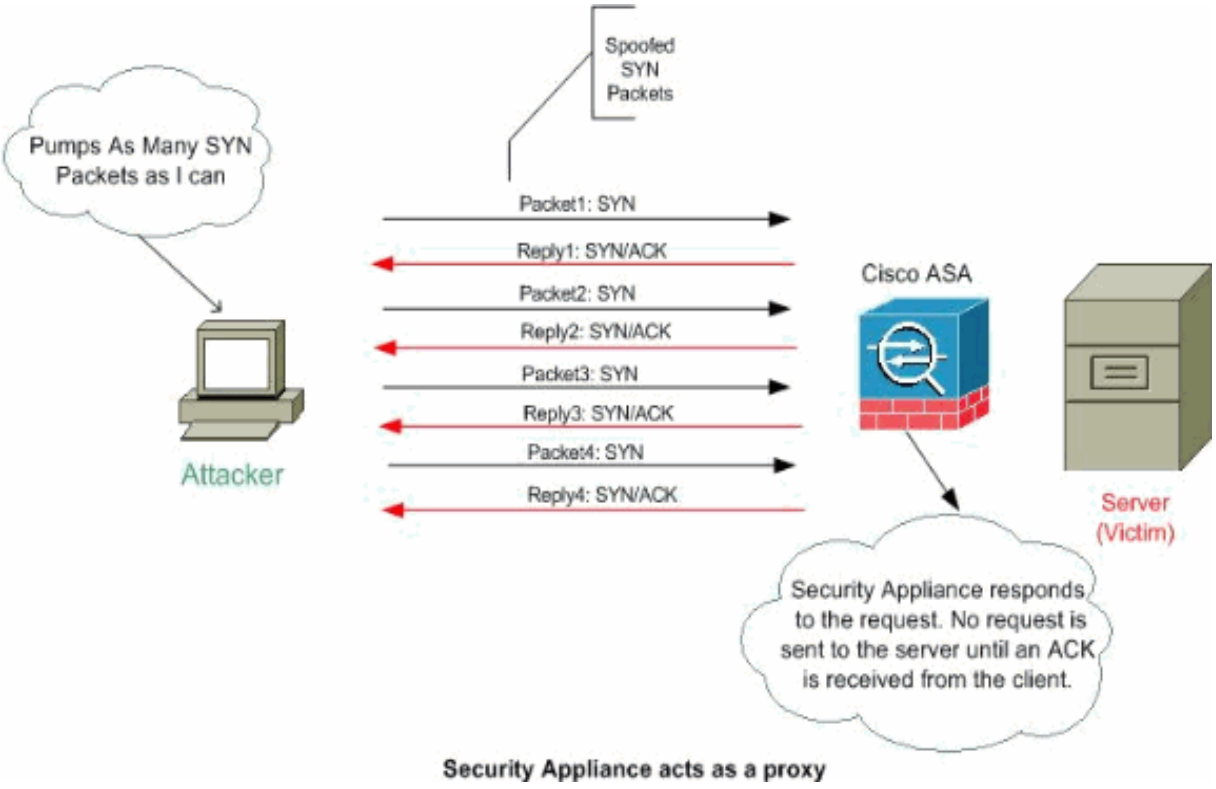



**Figure 4.1:** SYN Proxy protection in Cisco ASA 5510 [72]

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 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 65535. 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**}}

Command used for TCP-SYN Protection: NRL(config-pmap-c)# **set connection embryonic-conn-max** 1000

If the embryonic connection limit is reached ASA 5510, then the Cisco ASA 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 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.

### 4.1.2 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 [18-20].

Command used for limit UDP flood connections: NRL(config-pmap-c)# **set connection embryonic-conn-max** 1000

Cisco ASA 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 enabling the UDP flood protection feature, once threshold level is exceeded, it invokes the UDP flood attack protection feature [72]. 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.

### 4.1.3 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 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 [72]. 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.

### 4.1.4 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.

### 4.2 Experimental setup

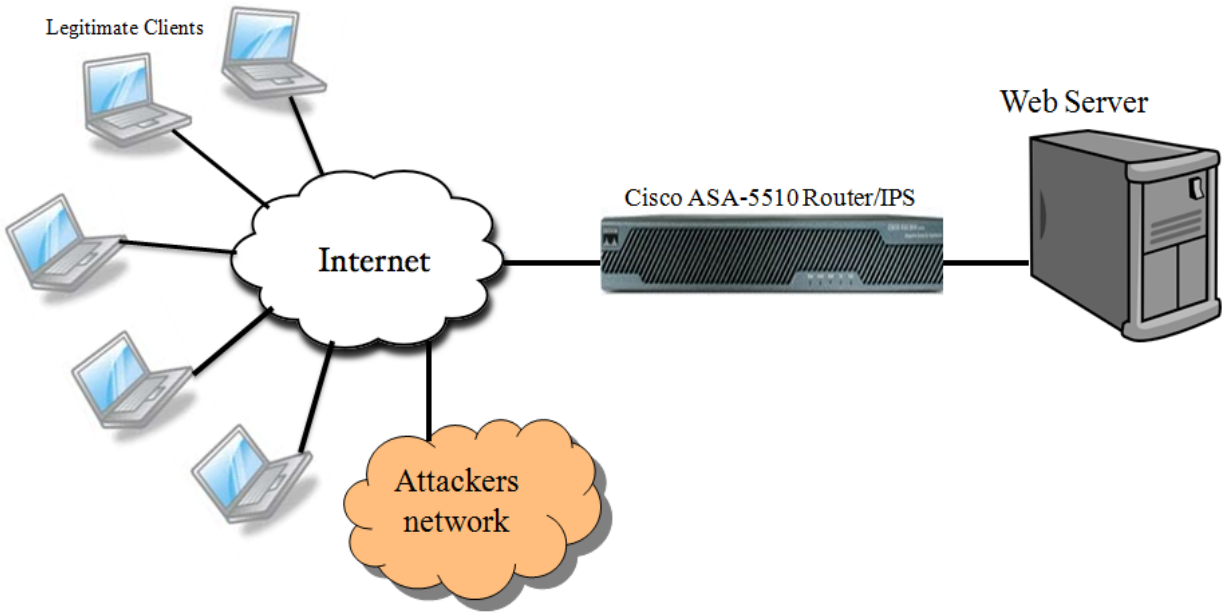



**Figure 4.2:** Experimental setup

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® Xeon™ 3GHz Processor with 4GB RAM are considered.

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 1Mbps to 100Mbps 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 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 Router/IPS in defending the common DoS attacks in the Internet.

## 4.3 Results and discussions

### 4.3.1 Performance of Cisco ASA 5510 Router/IPS under TCP-SYN Flood attack

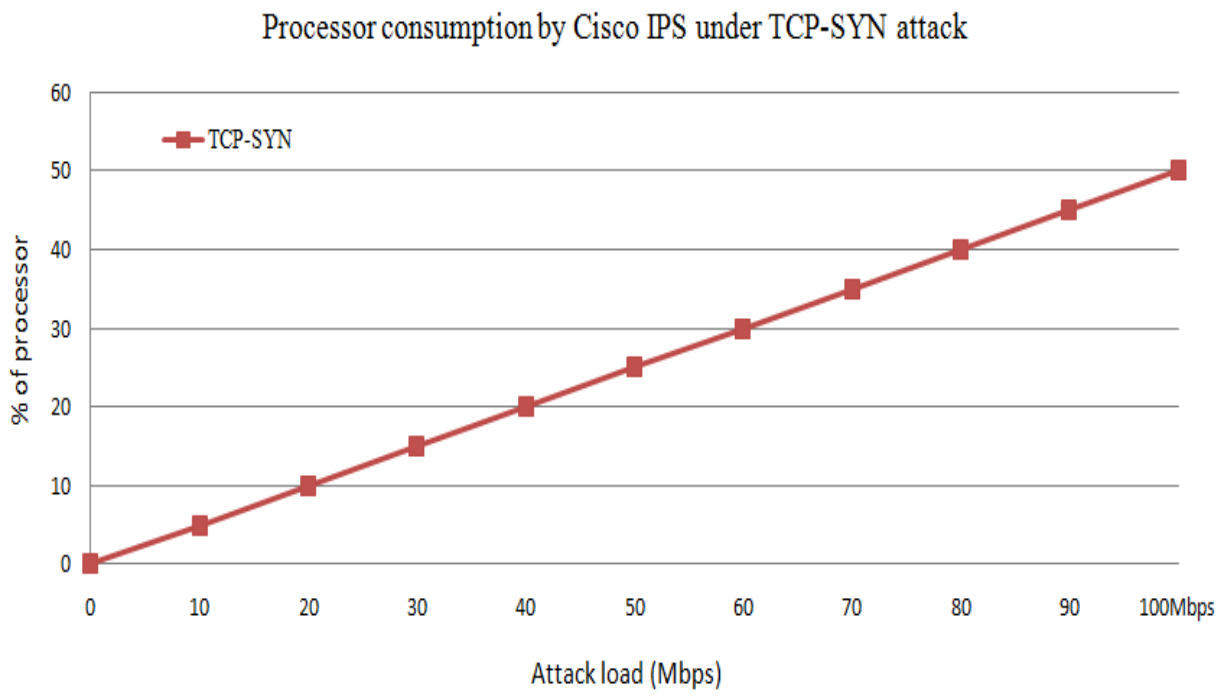
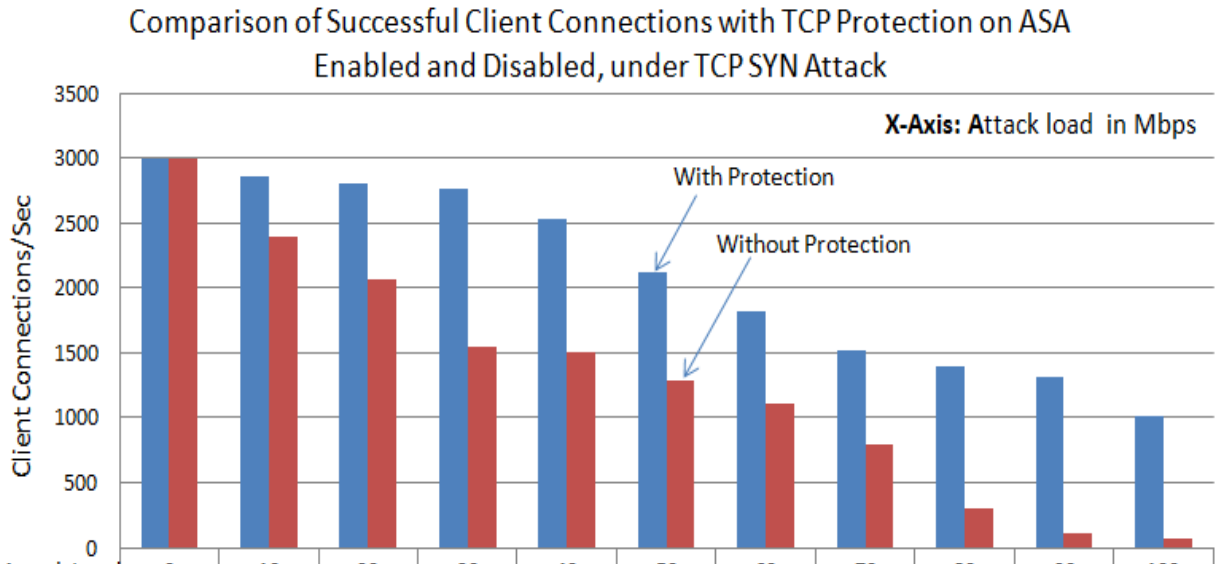



**Figure 4.3:** Processor consumption by Cisco IPS under TCP-SYN attack

**4.3.1.1 Processor consumption by Cisco ASA under TCP-SYN without legitimate traffic.** From the figure 4.3, it is observed that the processor consumption increases rapidly to 30% at 60Mbps TCP-SYN attack load and then 50% at 100Mbps attack load. The rapid 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 following section.

#### 4.3.1.2 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 100Mbps 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 100Mbps TCP-SYN attack load are 1012 per second. When there is no protection on the ASA, at 10Mbps attack load, successful connections recorded are 2,394, and with protection the number improved to 2,809. At 60Mbps attack load, without protection successful connections are brought down to 1,103 per second, which is improved by setting the threshold limit for embryonic connections records as 1,821 connections per second (Figure 4.4).




| 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 4.4:** Successful client 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.

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.

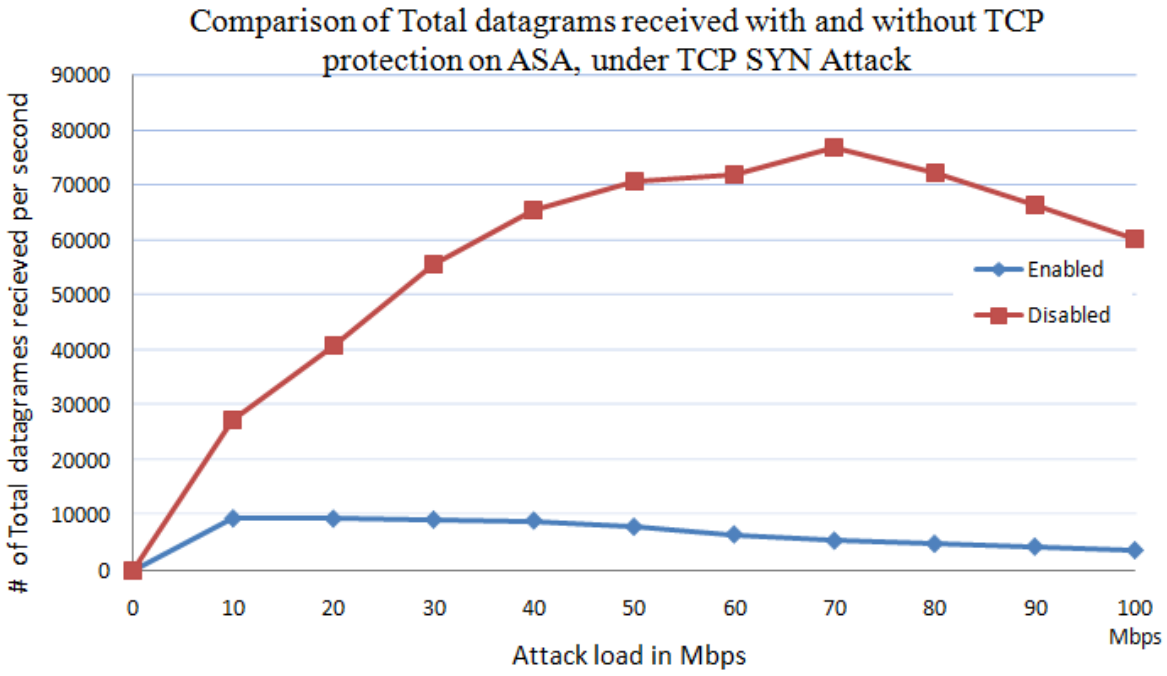



**Figure 4.5:** Comparison between total number of datagram's received by the web server at the time of ICMP Protection enabled and disabled on the web server.

From figure 4.5, 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 1Mbps attack load. The datagrams are rapidly increases and reaches to 29,000 at 10Mbps attack load, and then to the maximum of 77,000 datagrams at 70Mbps attack load. However at 1Mbps attack load, the web server is forming 3,000 connections per second (Figure 4.14) 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 4.3).

In case, with the TCP protection enabled on the Cisco ASA, when the attack traffic reaches the threshold limit 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 4.4) it is observed that only 10,000 datagrams are received by the IPS stably upto 10Mbps 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 1,012 connections per second at 100Mbps attack load.

### 4.3.2 Performance of Cisco ASA 5510 Router/IPS under UDP Flood attack

#### 4.3.2.1 Processor consumption by Router/IPS under UDP Flood attack without legitimate traffic.

From the figure 4.6, it is observed that the processor consumption reaches to 96% at 100Mbps UDP-Flood attack load. It is rapidly increasing, with 65% at 40Mbps attack load to 85% at 80Mps attack load. The rapid 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 show the influence of attack on the number of legitimate connections are in the fallow section (Section 4.3.2.2).

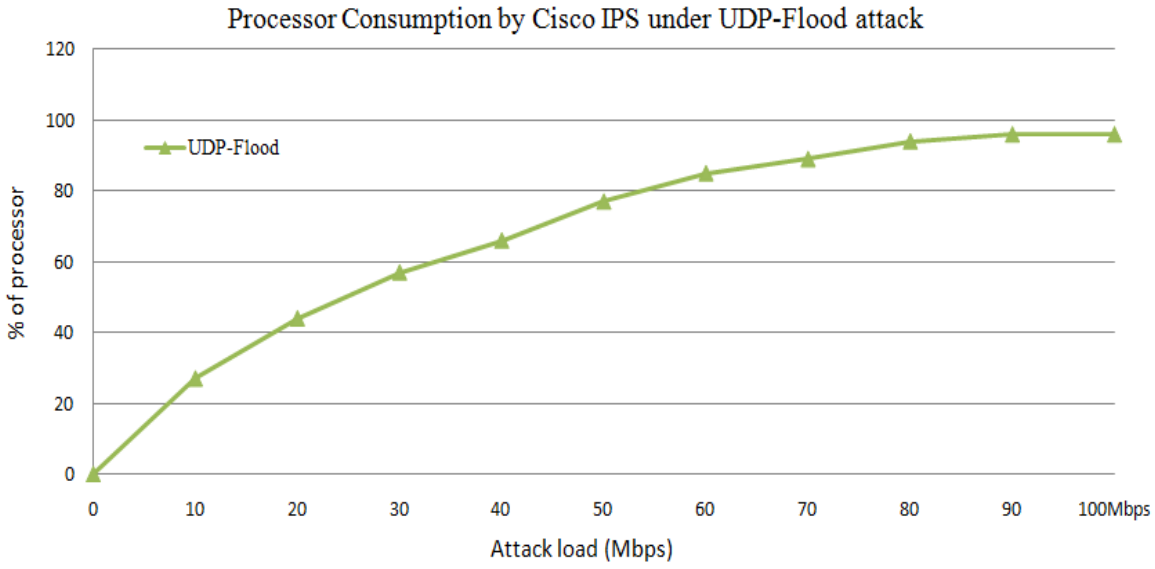
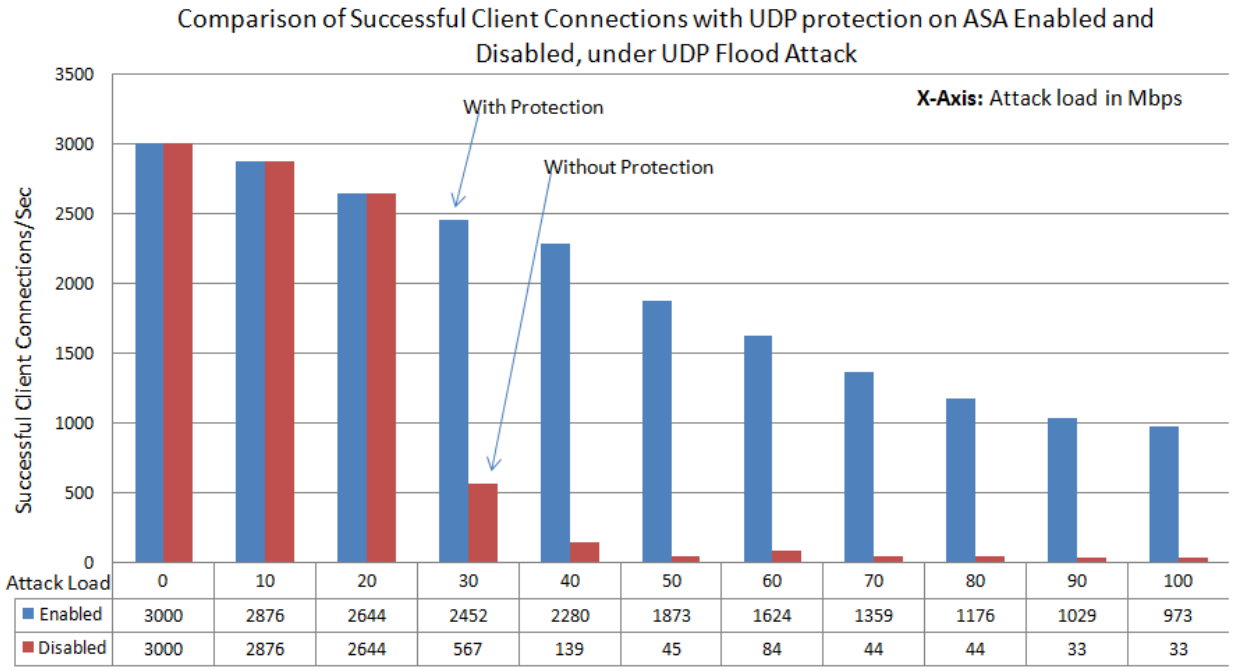



**Figure 4.6:** Processor consumption by Cisco IPS under UDP-Flood attack

#### 4.3.2.2 Performance of Cisco ASA under UDP-Flood attack along with the legitimate connections.

From this experiment (Figure 4.7), it is observed that the legitimate connections are drops to almost zero (less than 50 connections) under UDP flood attack load of 50Mbps 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 100Mbps 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 100Mbps attack load (Figure 4.7).




| 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 4.7:** Successful client 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.

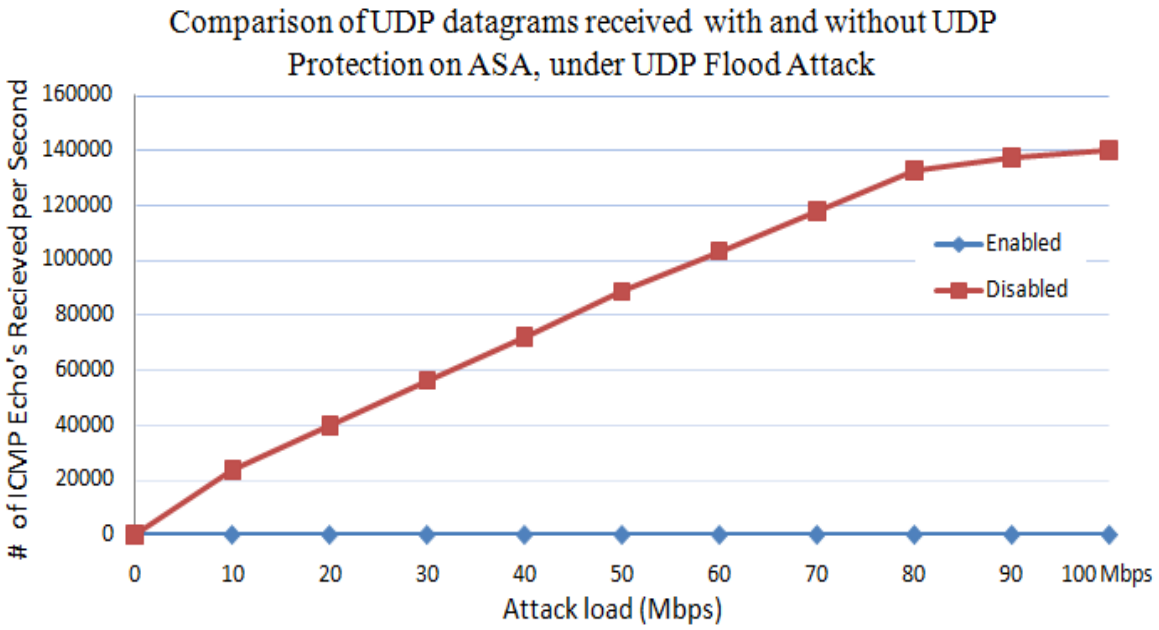



**Figure 4.8:** Comparison of UDP datagrams received by web server at the time of UDP Flood Protection enabled and disabled on the Cisco ASA.

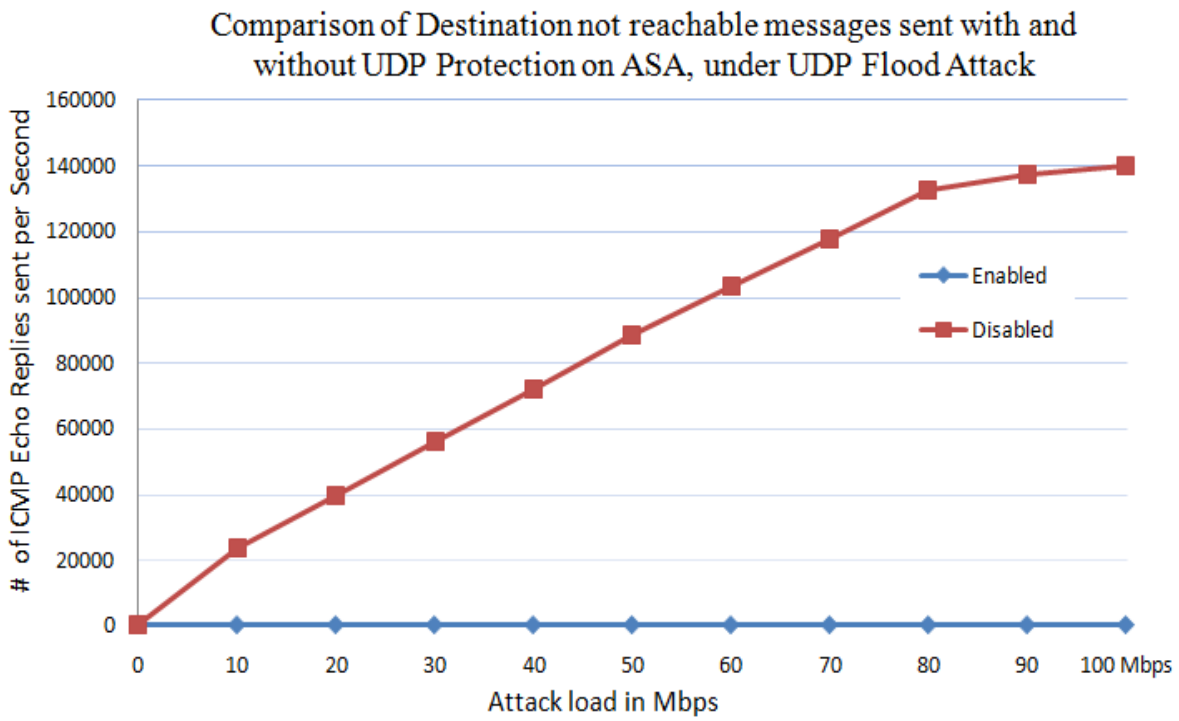



**Figure 4.9:** Comparison of Destination not reachable messages sent by web server at the time of UDP Flood Protection enabled and disabled on Cisco ASA.

From figures 4.8 and 4.9, it is observed that when the UDP protection is not enabled on the ASA, maximum of 1,40,000 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 4.8 and 4.9 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.

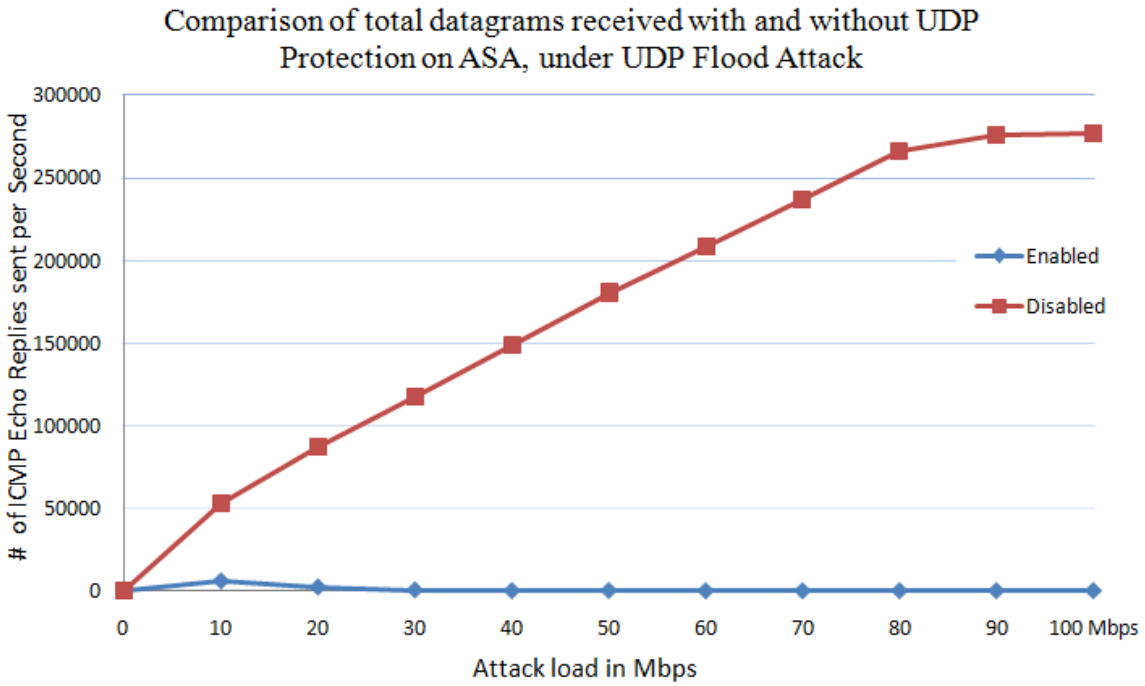



**Figure 4.10:** Comparison between total number of datagrams received by the web server at the time of ICMP Protection enabled and disabled on the web server.

From figure 4.10, it is observed that the maximum number of total datagrams received by the web server are 1,40,000 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.

### 4.3.3 Performance of Cisco ASA 5510 Router/IPS under ICMP PING attack

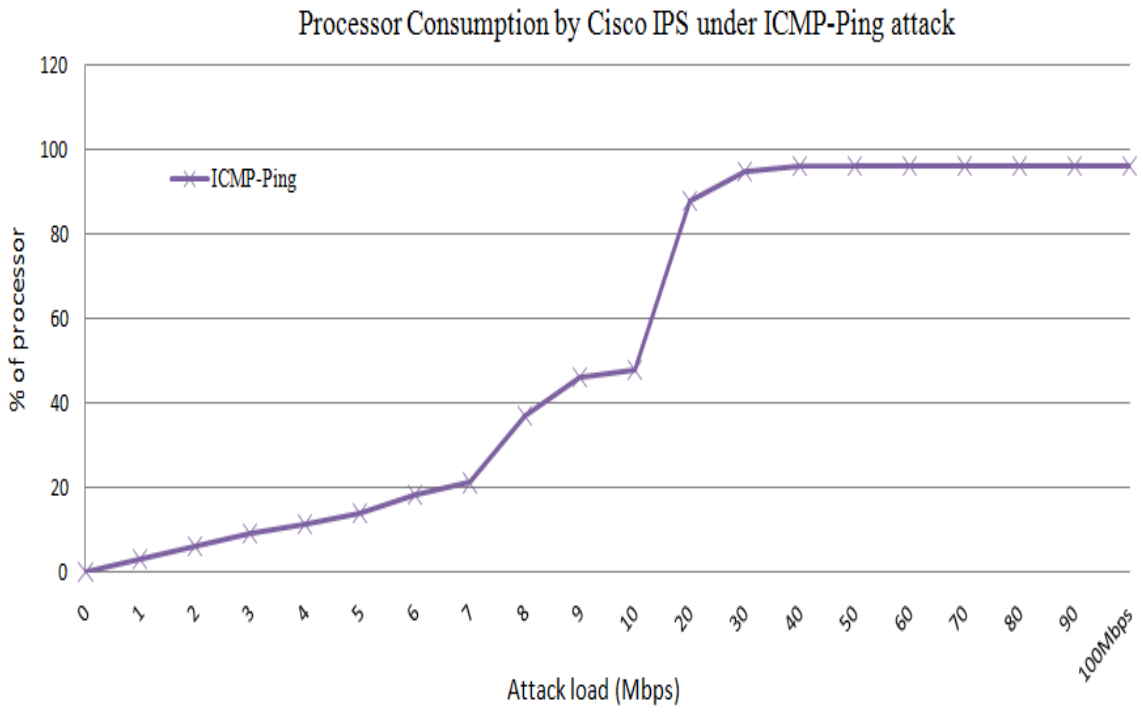
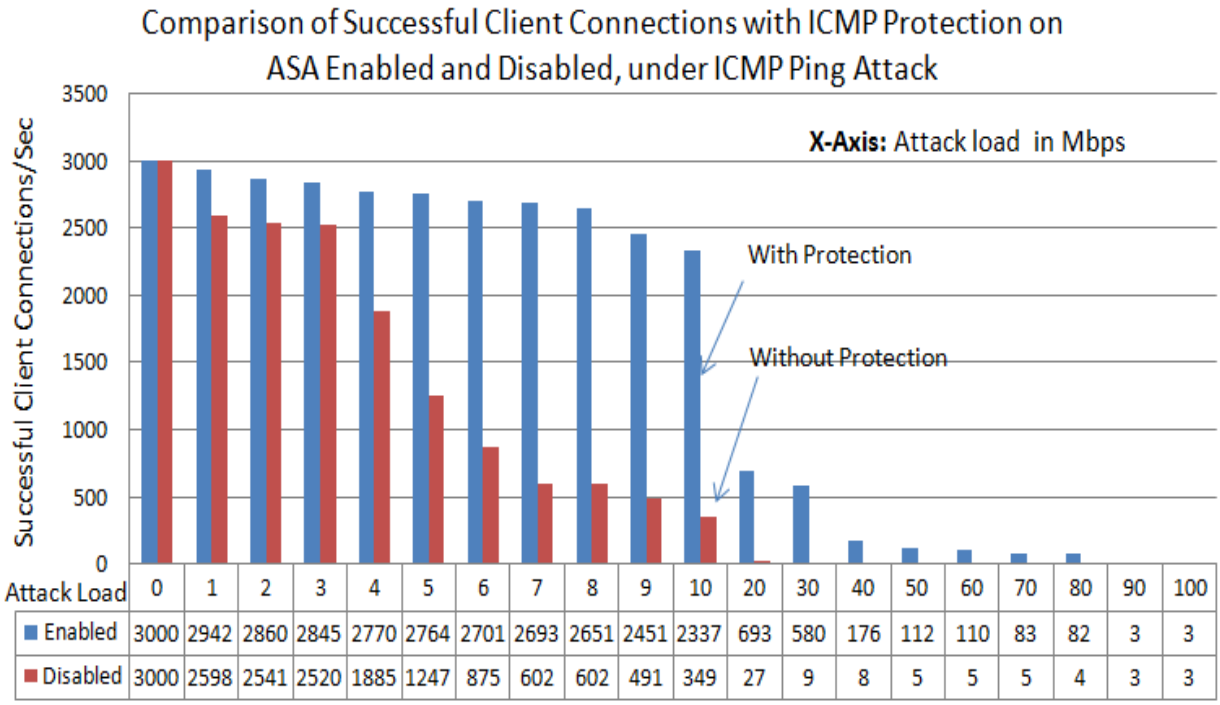



**Figure 4.11:** Processor consumption by Cisco IPS under ICMP-Ping attack

**4.3.3.1 Processor consumption by ASA under ICMP-PING attack without legitimate traffic.** From the figure 4.11, it is observed that the processor consumption reaches to 97% at 30Mbps 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.

#### 4.3.3.2 Performance of Cisco ASA under ICMP-PING attack along with the legitimate connections.

From these results (Figure 4.12), 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 20Mbps 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 40Mbps 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 4.12).




| 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 4.12:** Successful client 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.

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.

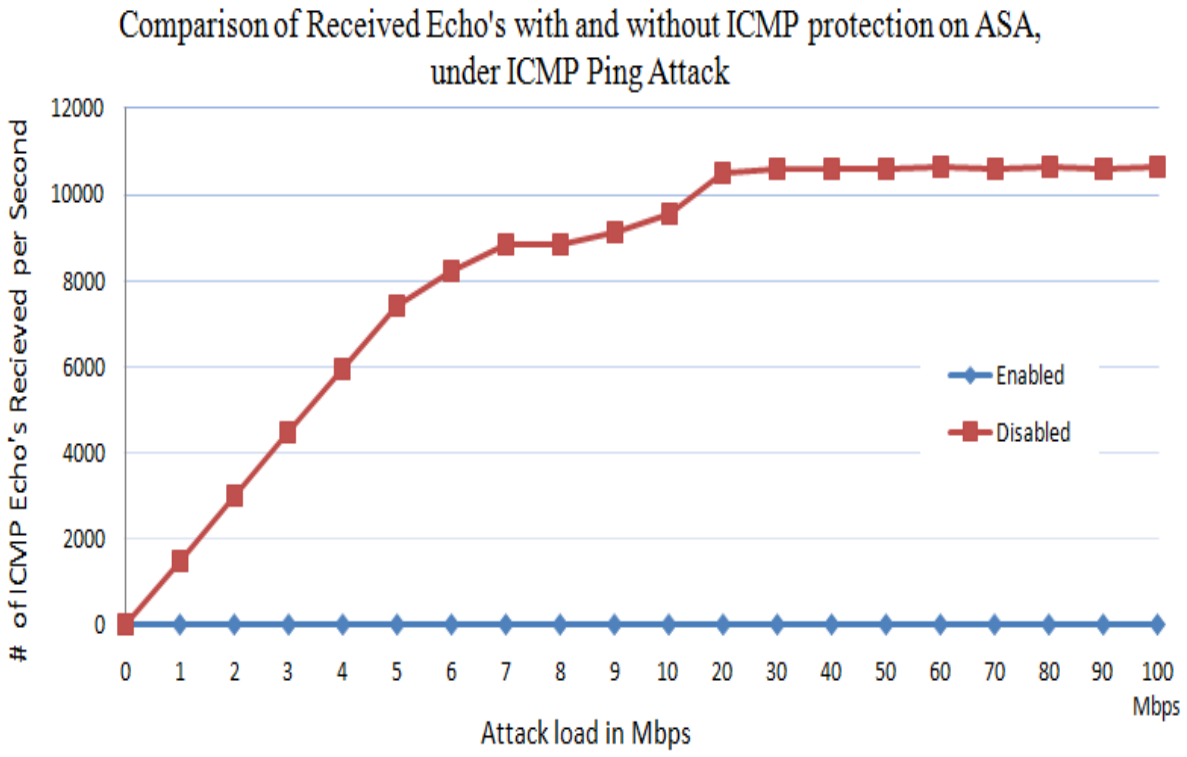



**Figure 4.13:** Number of ICMP echo's requests received by the web server with and without of ICMP Protection on the Cisco ASA-IPS.

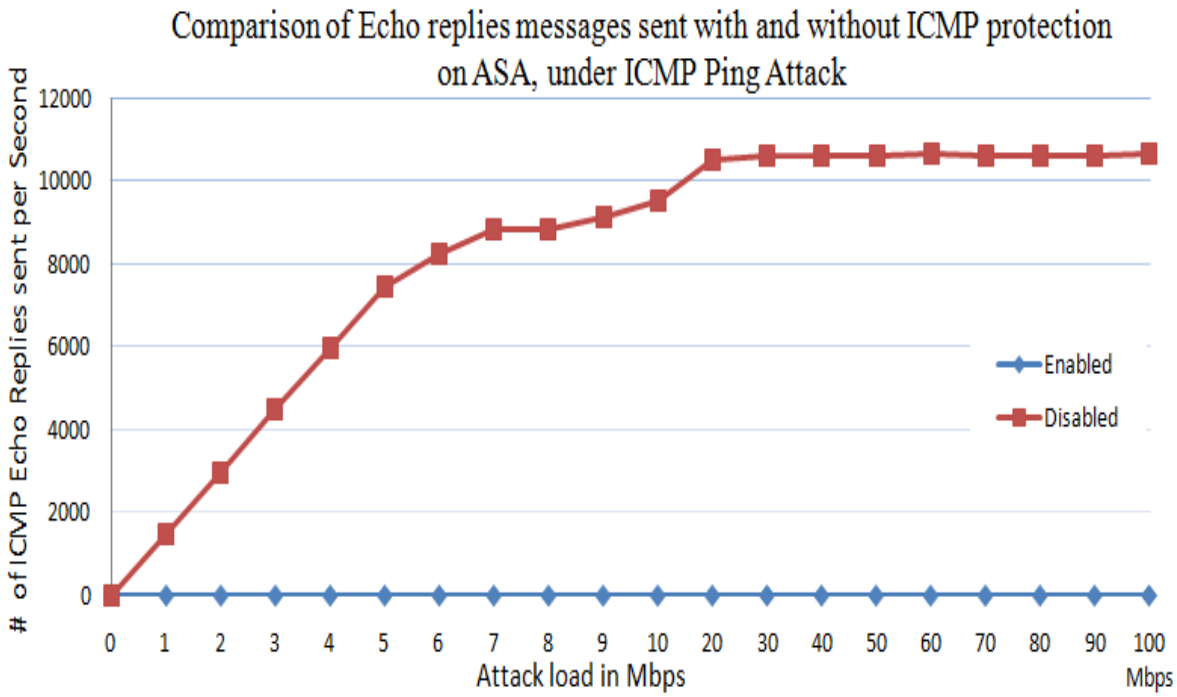



**Figure 4.14:** Number of ICMP echo's replies sent by the web server with and without of ICMP Protection on the Cisco ASA-IPS.

From figure 4.13 and 4.14, 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 4.13 and 4.14, 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.

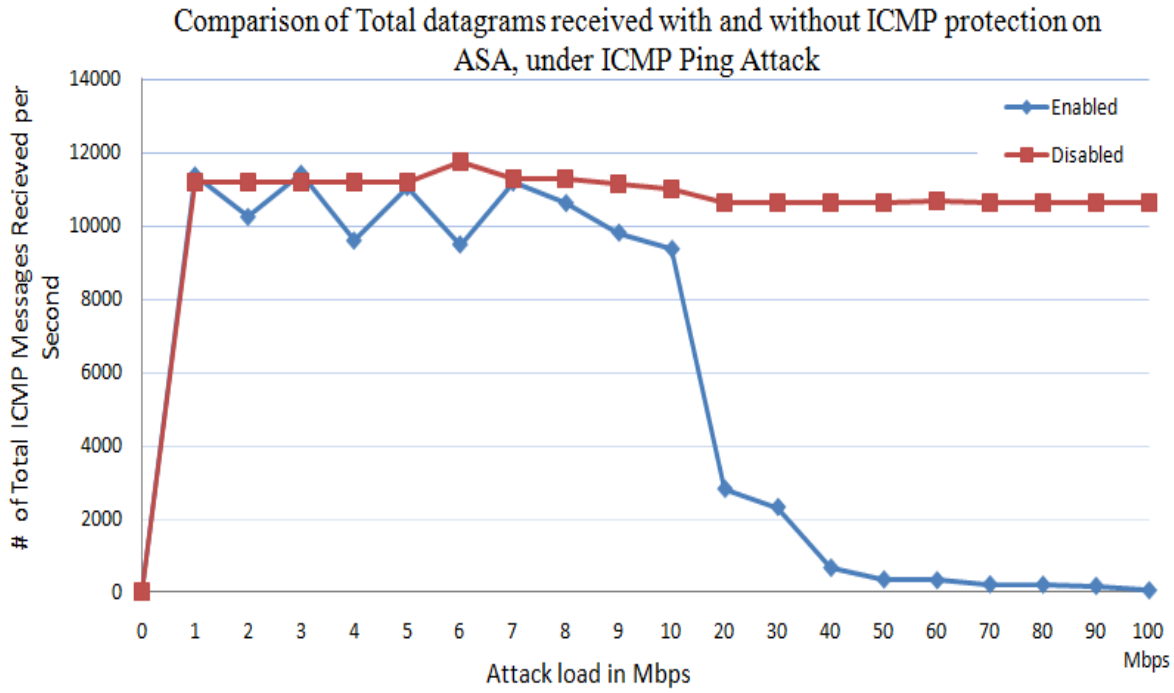



**Figure 4.15:** Total number of datagrams received by the web server with and without ICMP Protection enabled on Cisco IPS.

From figure 4.15, it is observed that the number of total datagrams received by the web server are stable after 20Mbps attack load at 11,000 connections per second without ICMP protection. However from figure 4.13, the total ICMP echo's received by the web server, which are attack packets, are around 10,500 after 20Mbps of attack load. This explains that the packets reaching the serve after the 20Mbps 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.

### 4.3.4 Performance of Cisco ASA 5510 Router/IPS under ICMP Land attack

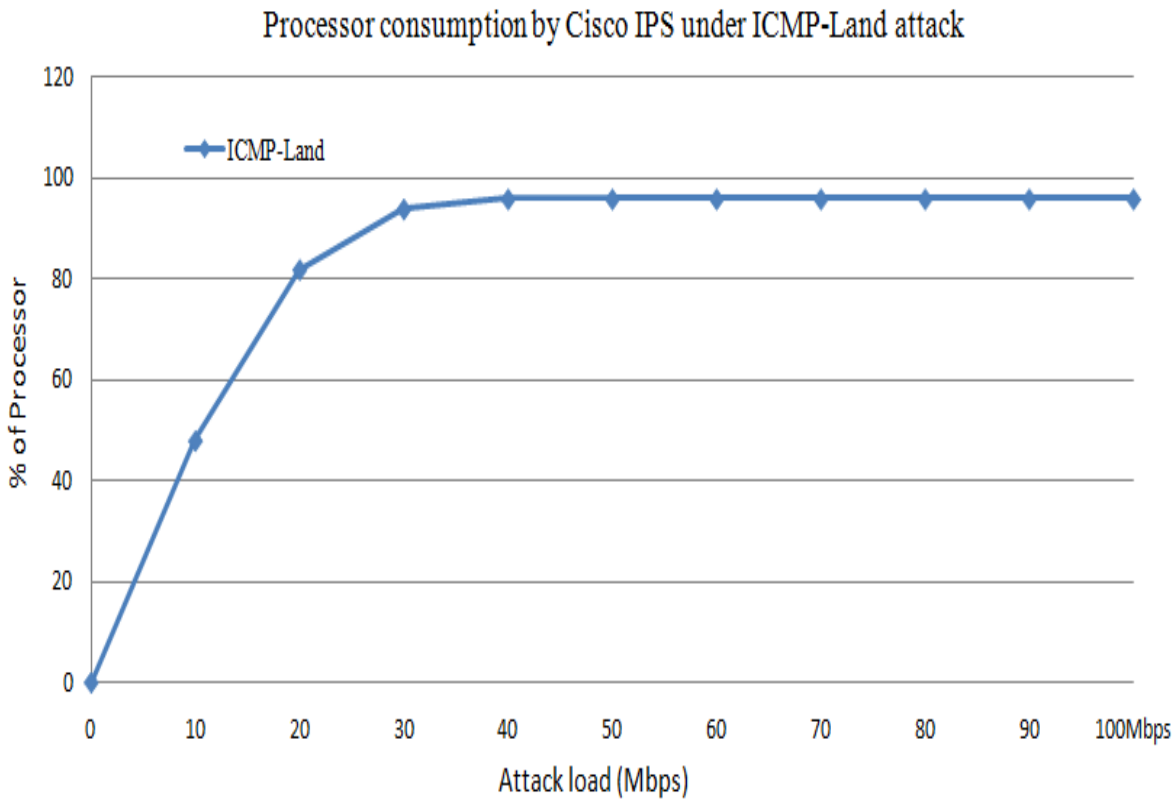



**Figure 4.16:** Processor consumption by Cisco IPS under ICMP-Land attack

**4.3.4.1 Processor consumption by Cisco ASA under Land attack without legitimate traffic.** From figure 4.16, it is observed that the processor consumption reaches to 97% at 30Mbps 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.

#### 4.3.4.2 Performance of Cisco ASA under ICMP-Land attack along with the legitimate connections.

From this experiment (Figure 4.17), it is observed that the legitimate connections are brought down to 700 under ICMP Land attack load of 40Mbps with default Land Attack protection enabled on the ASA. The number of connections are brought down to 633 at land attack load of 60Mbps, and at 100Mbps 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.

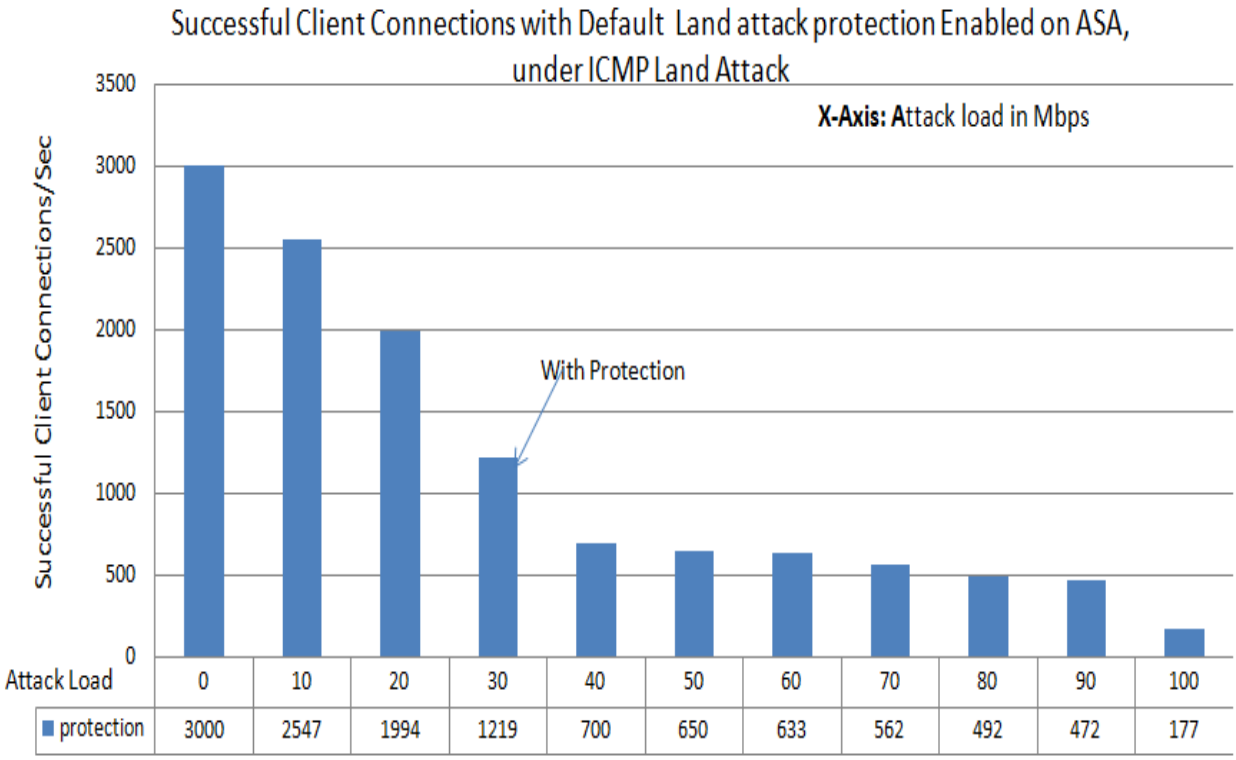



**Figure 4.17:** Successful client Connections formed with web server under ICMP Land attack, at different attack loads, with ICMP Land attack security enabled by default on the Cisco ASA

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 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.

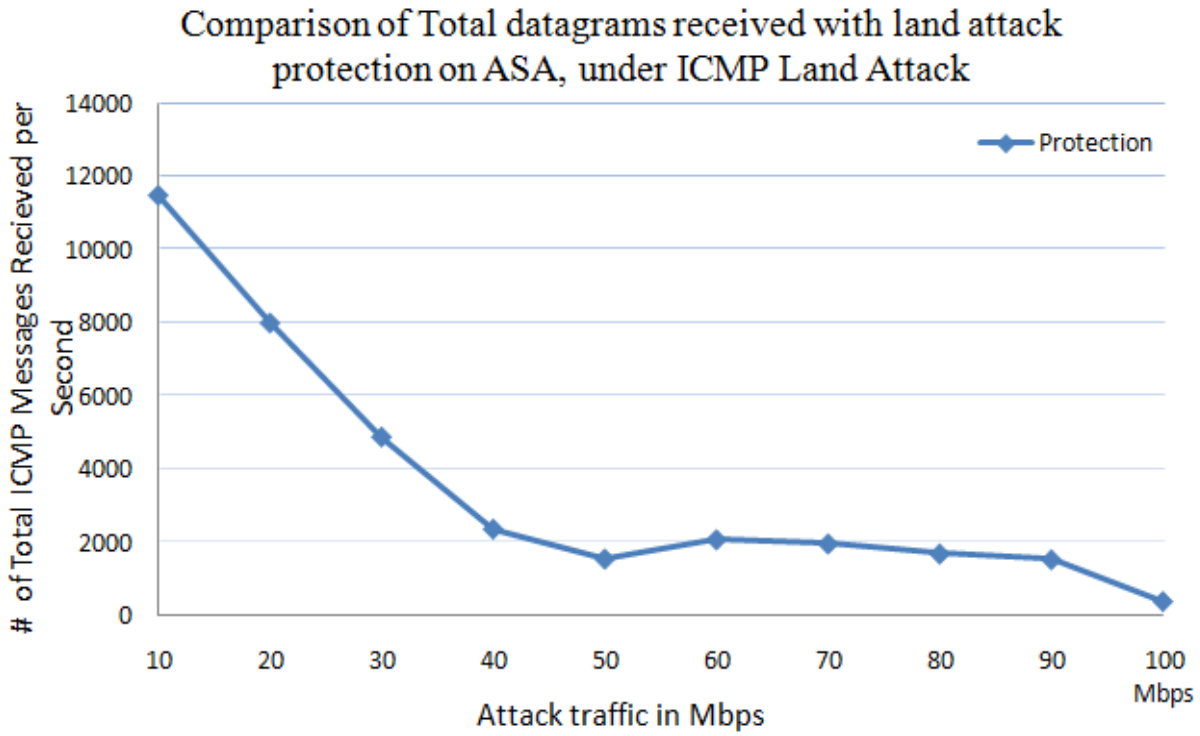



**Figure 4.18:** Comparison between total number of datagrams received by the web server at the time of ICMP Protection enabled and disabled on the web server.

From figure 4.18, it is observed that the number of total datagrams received by the web server are almost 12,000 per second upto the 20Mbps 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 40Mbps 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 4.16) for the legitimate traffic. This lead to no service for most of the clients, after reaching 40Mbps attack traffic (Figure 4.17).

## 4.4 Performance of the Web Server under DoS attacks having protection at Cisco ASA 5510 Routers/IPS and Servers together

The performance of the Web Server can be improved by protecting on the Host using Windows Firewall and also at Network level by using Cisco ASA 5510 routers/IPS's. The bandwidth capacity of the Windows server is 1 Gbps, where Cisco Router/IPS is having 100Mbps bandwidth. To protect this server with 1 Gbps link rate with Cisco Router/IPS, we can use multiple Cisco ASA-5510 Routers/IPS that supports a link bandwidth of 100Mbps each.

From figure 4.19, the traffic outside the private network, which is combination of legitimate clients and attack traffic, is passed through the De-Multiplexer. De-Multiplexer distributes the load towards the ten Cisco ASA IPS's. Cisco ASA/IPS prevents attack traffic from reaching the server. The filtered legitimate client traffic is then multiplexed back to 1 Gbps by another Multiplexer (figure 4.19). This multiplexed traffic is forwarded to the Web Server that supports 1 Gbps interface. On Web Server limited protection is provided by the Host based Microsoft Firewall, which was not sufficient in defending the DoS attacks by itself.

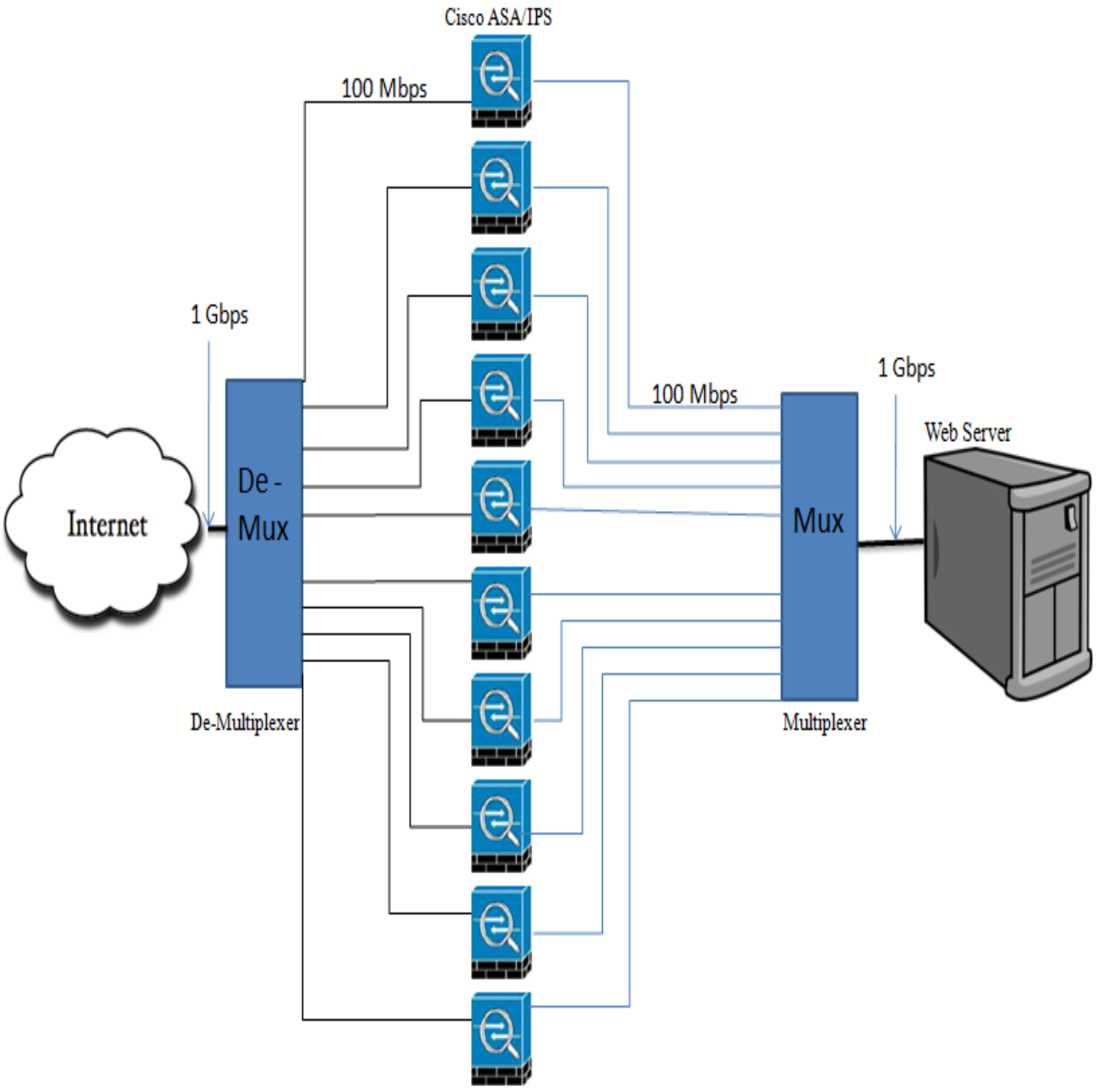



**Figure 4.19:** Web Server with protection on Host and also in the Network using Windows Firewall and Cisco ASA Router/IPS

### 4.4.1 Expected Improvement in the performance of the Web Server using this scheme

In the table below, we show performance improved by using this scheme.

| | Attack Type | Attack Load where number of client connections are zero with protection only on Server 2003 | Number of successful client connections | |
|---|---|---|---|---|
| | | | With protection on Server (Microsoft Firewall) | With protection on Server (Microsoft Firewall) and protection on Cisco ASA/IPS |
| 1 | TCP-SYN | 6 Mbps | 0 Connections | 20,000 Connections |
| 2 | UDP-Flood | 400 Mbps | 0 Connections | 20,000 Connections |
| 3 | ICMP-Ping | 400 Mbps | 0 Connections | 1,760 connections |
| 4 | ICMP-Land | 500 Mbps | 0 Connections | 6,500 Connections |

**Table 4.1:** Improvement in the performance of web Server with Security on both Host and Network side

From Table 4.1, it was observed that the number of successful client connections were brought down to zero at the attack load of 6 Mbps under TCP-SYN attack. In this case, there was only protection on the Host side. However with the protection on both server and network sides, the number of client connections can be improve up to 20,000 Connections per second under 6 Mbps SYN attack load.

Under UDP-Flood attack with the protection on host itself, the client connections were brought down to zero under the attack load of 400 Mbps. But these client connections can be improve up to 20,000 connections per second, with protection provided by new scheme in figure 4.19, at the same UDP-Flood attack load.

At 400 Mbps ICMP-Ping attack load with protection only on the host side, the client connections were recorded as zero. With protection provided by new scheme in figure 4.19, they can be improve upto 1,760 connections per second, under same 400 Mbps Ping attack load.

When server with only protection on host is attacked with 500 Mbps of ICMP-Land attack, it records zero client connections. At the same land attack load, if the protection was provided by new scheme in figure 4.19, it can be improve the performance of the Web server with 6,500 connections per second.

## 4.5 Chapter Summary

The Cisco ASA-5510 Router/IPS has built in security features for defense against Denial of Service attacks and was tested for its performance under DDoS attacks .The performance of the Router/IPS in protecting the web server against DDoS Attacks was observed in this chapter. As Cisco is one of the leading manufacturers in security systems we selected this Router/IPS for our experiments. It was tested against DDoS attacks such as TCP-SYN Flood, ICMP-Ping Flood, ICMP-Land and UDP-Flood attacks. The maximum number of stable client connections formed with the web server was 3,000 connections/ second. There were two scenarios for all the DDoS attacks; with the protection enabled on ASA and protection disabled on ASA.

When the ICMP-Ping flood attack was sent towards the web server through IPS, without any protection enabled on the IPS, it was observed that there were almost zero connections at 20Mbps attack load. However, with ICMP protection enabled on the IPS, number of connections drops to almost zero at 40 Mbps of attack traffic load. This shows improvement with the protection on the IPS, but after 40Mbps 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 land attack packets were blocked by default. Under this attack, the connections were found to be almost zero at 90 Mbps of attack traffic load. 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. Under TCP-SYN attack without protection, the connections were brought down to almost zero at 80Mbps 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. Under UDP flood attack without protection, the numbers of successful connections were around 500. And with protection it was improved to around 2,500. At 90Mbps UDP flood attack traffic without protection, the connections observed were 33, with protection this was improved to 1000 connections per second.

In the scenario with protection on the both server and Cisco ASA (figure 4.19) were enabled, it was observed that the number of stable client connections improved compared to case when protection is only on the server itself. At 6 Mbps of SYN attack load it can form 20,000 connections per second were in other case it resulted as zero connection. At 400Mbps UDP-Flood attack load it was improved to 20,000 connections per second from zero connections. Under 400Mbps Ping attack, it was recorded as 1,760 connections with the latest scenario (figure 4.19) which should be zero connections per second with protection only on the server. And, also under 500Mbps Land attack, it was improved from zero connections to 6,500 connections per second.

# CHAPTER V

# CONCLUSIONS AND FUTURE WORK

In this thesis, testing of server operating systems and some selected firewalls/IPS along with their built in security capabilities was done to evaluate how secure these systems were against DDoS attacks. Servers considered for this thesis were- Windows Server 2003 and windows Server 2008. Also security systems like Juniper networks Netscreen 5GT firewall and Cisco ASA-5510 IPS are tested under common DoS attacks to investigate the security provided by them from DoS attacks and also availability provided by them at the same time.

In chapter 2, it was found that the most popular server operating systems, Microsoft Windows server 2003 and Windows server 2008 were not robust enough against TCP-SYN attack. These servers were not able to handle to TCP-SYN attack even at lower attack loads with default SYN protection enabled on the servers. They were not able to provide availability under other common DoS attacks such as ICMP-Ping flood attack, ICMP-land attack and UDP-Flood attacks, which resulted in zero successful legitimate connection at the higher loads of attack traffic on 1Gb link rate. Windows server 2003 forms a maximum of 20,000 successful stable client connections and Windows server 2008 forms 25,000 successful stable client connections per second. However under TCP-SYN attack, windows 2003 server resulted in zero legitimate connections due to 100% processor consumption at lower attack loads of 6 Mbps. Server 2008 was crashed at 6 Mbps attack load due to depletion of memory resources, resulting in zero

successful connections. Other common DoS attacks has also resulted in zero legitimate successful connections at the higher attack loads due to consumption of critical resources on these servers such as processor, memory and bandwidth. When compared ,Windows 2003 was defending well than newly released Microsoft windows 2008 server in terms of availability.

Juniper networks Netscreen 5GT firewall/IPS , which is a stateful firewall/IPS along with security features to defend against DoS attacks, is tested under common DoS attacks in Chapter 3. The maximum number of stable client connections formed with the server through the firewall/IPS was 600 connections per second. When the firewall was stressed with TCP-SYN attack traffic, it was able to sustain up to 40Mbps of attack traffic load and there after the connection rate was found to be zero with the SYN-proxy protection enabled on the firewall. Without the SYN-proxy protection the connection rate was found to be zero at 20 Mbps of attack traffic load. It was also observed that the connection rate was zero after 30Mbps attack load of ICMP-Ping attack, with ICMP-Ping flood attack protection enabled on firewall. Under ICMP-land attack, with land attack protection legitimate users were not able to use the services at land attack load of 45Mbps load. With UDP-flood attack load of 45 Mbps with UDP-Flood protection enabled on the firewall, client connections were zero. There was an improvement in connection rate when the protection was enabled in all the cases; however this improvement in performance was of not much use as the availability of the server to its hosts is zero at such low attack loads. This was due to the consumption of resources on firewall in processing and defending against illegitimate traffic.

The evaluation of popular Cisco ASA-5510 router with intrusion prevention system under common DoS attack was analyzed in the Chapter 4. As Cisco is the one of the leading manufacturer in security systems we selected this for our experiments, and stress tested under

common DoS attacks such as TCP-SYN Flood, ICMP-Ping Flood, ICMP-Land attack and UDP-Flood attack to evaluate security performance. The maximum number of stable client connection rate formed with the server was 3,000 connections per second. When the ICMP-Ping flood attack was sent towards the server through IPS, with ICMP protection enabled on the IPS, it resulted in zero legitimate client connections at 90 Mbps of attack load. By default, Cisco ASA router/IPS provided protection against land attack. Under this attack, the connections were dropped down to 472connections per second at attack load of 90 Mbps, which was due to the overhead in processing all the packets and verifying with the default security features to find the illegitimate traffic and drop them. Under TCP-SYN attack without protection, the connections were brought down to 307 connections at 80Mbps attack load. However by enabling SYN protection with threshold limit for embryonic connections as 100, improvement in the number of connections was observed. Under UDP flood attack without protection, the numbers of successful connections are around 500 and with protection it is improved to around 25,000. At 90Mbps UDP flood attack traffic without protection, the connections observed are 33, however with protection which is improved to 1000 connections per second. In the scenario with protection on the both server and Cisco ASA were enabled, it was observed that the number of stable client connections improved compared to case when protection is only on the server itself.

The analysis and discovery of the performance of popular server operating systems and also the famous security systems will be helpful for the network administrators, who maintain the major and sensitive networks, to analyze their resources in reaching the security requirements to satisfy their legitimate users. These results were also helpful for the manufactures, in building their devices that meet the security and availability requirements in considering the effects of denial of Service attacks that are causing great disruptions in the current days. Results from this

thesis were also helpful for researchers and engineers who are working on the defensive mechanisms for Denial of Service attacks, in improving the features and decrease the over head on the systems. These results will also be helpful in understanding the need for proper testing of these products before they were released and ready for use to general public.

The future work of this thesis will be to study the vulnerabilities of different server operating systems like Linux and UNIX which are used all over the world. Network security systems with latest technology and features can also be tested under Denial of Service attacks and their performance can be evaluated. Host based Intrusion prevention systems for the servers, can also be tested. Different security options can be tested when they are enabled all at once. Also, different DoS attack packets can be combined as to design the real-time traffic and such a barrage can be forwarded to the server and its performance can be evaluated. Also the security loop holes in IPv6 can be tested.

## REFERENCES


[1] “US suspects N Korea launched Internet attack on July 4” is available online at (http://ibnlive.in.com/news/us-suspects-n-korea-launched-internetattack-on-%20%20%20%20%20july-4/96715-2.html) July 9 2009.

[2] US, S. Korean websites under attack; available online at (http://government.zdnet.com/?p=5093) last access on: July-27, 2010.

[3] Latest DDoS attack on twitter available online at (http://status.twitter.com/post/157191978/ongoing-denial-of-service-attack) last access on: July-27, 2010.

[4] Latest DDoS attack on twitter and Facebook available online at (http://www.techcrunch.com/2009/08/06/ddos-attacks-crush-twitter-hobble-facebook/) last access on: July-27, 2010.

[5] “Arbor Networks Releases fifth Annual Infrastructure Security Report” available online at (http://www.arbornetworks.com/en/arbor-networks-releases-fifth-annual-infrastructure-security-report-2.html).

[6] “Fact Sheet: Root server attack on 6 February 2007,” Available at (www.icann.org/en/announcements/factsheet-dns-attack-08mar07.pdf*),* ICANN, Published on: March-1, 2007.

[7] Sharon Gaudin: Storm Botnet behind Canadian DoS Attack, available online at (http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=201500196 ) last access on: July-27, 2010.

[8] Sharon Gaudin: DoS Attack Cripples Internet Root Servers, available online at (http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=197003903) last access on: July-27, 2010.

[9] John D. Sutter, CNN, “Is WikiLeaks engaged in 'cyber war'? December 09, 2010, available at (http://articles.cnn.com/2010-12-09/tech/wikileaks.cyber.attacks_1_cyber-war-cyber-weapons-cyber-attacks?_s=PM:TECH), last access on: July-27, 2010.

[10] Lee Garber, Denial-of-Service Attacks Rip the Internet, IEEE Computer, v.33 n.4, p.12-17, April 2000.

[11] Y.Ohsita, S. Ata, M. Murata, ―Detecting Distributed Denial-of-Service Attacks by analyzing TCP SYN packets statistically, Global Telecommunications Conference, GLOBECOM '04, IEEE Volume 4, 29 Nov. - 3 Dec. 2004, On Page(s):2043 - 2049 Vol.4.

[12] Tian, H.-T., Huang, L.-S., Lei, Y.-F., and Chen, G.-L. A new scheme for IP traceback under DOS attack, Proc. 4th Int. Conf. on Parallel and Distributed Computing, Applications and Technologies, (PDCAT‘2003), 27–29 Aug. 2003, On Page(s): 189–193.

[13] Rocky K. C. Chang, ―Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial, IEEE Communications Magazine, Oct., 2002, Volume: 40 Issue: 10 On page(s): 42 - 51

[14] Sirisha Surisetty, Sanjeev Kumar, “Is McAfee SecurityCentre/Firewall Software Providing Complete Security for your Computer?” 2010 Fourth International Conference on Digital Society, (ICDS 2010), St.Maarten, Netherlands, February 10-16, 2010, On page(s): 178 – 181.

[15] Raj S, Hari V, Sanjeev Kumar: Performance of Windows XP, Windows Vista and Apple’s Leopard Computers under a Denial of Service Attack. IEEE International Conference on Digital Society, FEB-2010, On page(s): 188 – 191.

[16] J. Mirkovic and P. Reiher, ―A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communications Review, April 2004, Volume: 34(2), On page(s): 39-54.

[17] F.A. El-Moussa, N. Linge, and M. Hope, ―Active router approach to defeating denial-of-service attacks in networks, Communications, IET Volume 1, Issue 1, February 2007,On Page(s): 55 – 63.

[18] Yau, D.K.Y., Lui, J.C.S., Feng, L., and Yeung, Y, ―Defending against distributed denial of service attacks with max–min fair server-centric router throttles, IEEE/ACM Trans. Netw., 2005, 13, (1), On page(s): 29–42.

[19] Rocky K.C.Chang, Defending against flood based distributed denial of service attack –A tutorial, IEEE communication Magazine, Oct., 2002, Volume: 40 Issue: 10, On page(s): 42 – 51.

[20] Xu. Y, ―Statistically countering denial of service attacks, Proc. IEEE Int. Conf. on Communications (ICC 2005), 16–20 May 2005, vol. 2, pp. 844–849.

[21] Jelena Mirkovic, Sven Dietrich, David Dittrich and Peter reiher – Internet Denial of service: Attack and Defense Mechanism, Publisher: Prentice Hall, Copyright: 2005, Format: Paper; 400 pp, Published: 12/30/2004.

[22] D.Karig, and R. Lee, Remote Denial of Service Attacks and counter measures, Department of Electrical Engineering, Princeton University, Technical Report CE-L2001-002, October 2001.

[23] Christos Douligeris, and Aikaterini Mitrokotsa, DDoS attacks and Defense Mechanisms: Classification and state-of-art, Department of informatics, University of Piraeus, Computer Networks, Volume 44, Issue 5, 5 April 2004, Pages 643-666.

[24] P.Ferguson, and D.Senie, Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing, RFC 2827, 2001.

[25] Xianjun Geng and Andrew B.Whinston, Defeating Distributed Denial of Service Attacks, IEEE Computer Society, IT Professional, 2000, Volume: 2 Issue: 4, Pages: 36-42.

[26] R.R. Talpade, G. Kim, and S. Khurana, NOMAD: Traffic-based network monitoring framework for anomaly detection, Proceedings of the fourth IEEE symposium on computers and communications, 1999, pp. 442-452.

[27] Nathalie Weiler, Honeypots for Distributed Denial of Service Attacks, Computer Engineering and networks Laboratory, Swiss Federal Institute of Technology, Proceedings of the eleventh IEEE international workshops on enabling technologies, 2002, On page(s): 109 – 114.

[28] S. Kumar: Impact of distributed denial of service (DDoS) attack due to ARP storm, 4th International Conference on Networking (ICN), 2005, pp. 997-1002.

[29] J. Postel: Internet Control Message Protocol, DARPA Internet program protocol specifications, RFC 792, September 1981.

[30] Sanjeev Kumar: PING attack - How bad is it? Computers & Security Volume 25, Issue 5, July 2006, Pages 332-337.

[31] Wei Chen, Dit-Yan Yeung; Pi-E Liu: Defending Against TCP SYN Flooding Attacks Under Different Types of IP Spoofing, Ne International Conference on Networking Systems and International Conference on Mobile Communications and learning Technologies, 2006. ICN/ICONS/MCL 2006. 23-29 April 2006, pp. 38

[32] RFC 793 “Transmission Control Protocol”, is available online at (http://www.faqs.org/rfcs/rfc793.html ), last access on: July-27, 2010.

[33] TCP Three Way hand shake, available online at (http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-4/syn_flooding_attacks.html) last access on : July-27, 2010.

[34] W. Eddy, RFC 4987 “TCP SYN Flooding Attacks and Common Mitigations” available at (www.ietf.org/rfc/rfc4987.txt), last access on: July-27, 2010.

[35] “Transmission Control Protocol/Internet Protocol (TCP/IP)” available at (technet.microsoft.com/en-us/library/cc759700(WS.10).asxp) © 2010 Microsoft Corporation. Last access on: July-27, 2010.

[36] Cnet news, “Twitter crippled by denial-of-service attack” is available online at (http://news.cnet.com/8301-13577_3-10304633-36.html), August 2009.

[37] Pi-E Liu, Zhong-Hua Sheng: Defending against tcp-syn flooding with a new kind of syn-agent., International Conference on Machine Learning and Cybernetics, Volume 2, 12-15 July 2008 Page(s):1218 - 1221.

[38] Shakhov, Vladimir V. , Choo, Hyunseung: On modeling counteraction against TCP SYN flooding, 21st International Conference on Information Networking, ICOIN 2007, January 23, 2007 - January 25, 2007, Volume 5200/2008, On Page(s): 574-583.

[39] Sanjeev Kumar, Einar Petana: Mitigation of TCP-SYN Attacks with Microsoft’s Windows XP Service Pack2 (SP2) Software, Seventh International Conference on Networking, IEEE 2008, On page(s): 238 – 242.

[40] RFC 792 “Internet Control Message Protocol,” J Postel, September 1981 is available online at (http://www.faqs.org/rfcs/rfc792.html), last access on: July-27, 2010.

[41] S. Kamal and B. Issac, Analysis of Network Communication attacks, Research and Development, 2007. SCOReD 2007. 5th Student Conference Dec, 2007, On page(s): 1 – 6.

[42] Computer Emergency Response Team (CERT)® Advisory CA-2001-20. Home network security, is available online at (http://www.cert.org/tech_tips/home_networks.html), last access on: July-27, 2010.

[43] Dr. S Kumar, “Can Microsoft’s service pack 2 security software prevents Smurf attacks?” AICT-ICIW'06, IEEE computer society, Sep 2006, On Page(s): 89-95.

[44] Sanjeev Kumar: Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet, Second International Conference on Internet Monitoring and Protection (ICIMP 2007), pp. 25.

[45] “Impact of Land attack Compared for Windows XP, Vista and Apple Leopard”, award winning poster during HESTEC Science Symposium at The University of Texas – Pan American, Sep 2009.

[46] Computer Emergency Response Team (CERT)® “Trends in Denial of service attacks Technology” is available online at (http://www.cert.org/archive/pdf/DoS_trends.pdf) , last access on Dec-01-2009.

[47] “Register.com sufferes week-long DDoS attack on DNS servers” available at (http://www.secure64.com/news-register-reflective-ddos-dns)

[48] Shigang Chen, Yibei Ling, Randy Chow and Ye Xia” AID: A global anti-DOS service”, Computer Networks 51,May 2007, On page(s): 4252 - 4269.

[49] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic: Distributed Denial of Service Attacks. IEEE International Conference on Systems, Man, and Cybernetics, pages 2275-2280, Nashville, TN, USA, October 2000.

[50] Y.Chen, K.Wang, and W.Ku, Collaborative Detection of DDOS Attacks over Mutiple Networks, IEEE Transactions on parallel and distributed systems, 2007, Volume: 18 Issue:12, On page(s): 1649 - 1662 .

[51] Neumann Peter G ―Inside Risks: Denial of Service Attacks, Communications of ACM, Volume 43, Issue 4, April 2000, On page: 136.

[52] J.Xu and W.Lee, Sustaining availability of web services under distributed denial of service attacks, IEEE transactions on computers, Vol. 52, Feb., 2003, Volume: 52 Issue:2, On page(s): 195 - 208.

[53] Microsoft corp.," Microsoft technical support for windows server 2003 R2" http://technet.microsoft.com/en-us/library/cc756026.aspx

[54] John Fontana, Survey shows many companies have eye on Windows Server 2008; (http://www.networkworld.com/news/2008/021908-windows-server-2008-survey.html); February 19, 2008

[55] T.Berners-Lee, R.Fielding, H.Frystyk, "Hypertext Transfer Protocol—HTTP/1.0 ",RFC1945 ,May 1996.

[56] Intel Inc, "Intel Xeon® Quad core Processor" available at (http://www.intel.com/support/processors/xeon/), last access on: July-27, 2010.

[57] Ross Oliver, Tech Mavens; "Countering SYN Flood Denial of Service Attacks" Aug 29, 2001; available at (http://www.tech-mavens.com/synflood.htm), last access on: July-27, 2010.

[58] "Tuning TCP/IP Response to Attack" available at (technet.microsoft.com/en-us/library/cc759239(WS.10).aspx), updated on July 6, 2005, last access on: July-27, 2010.

[59] "TCP/IP Registry Values for Microsoft Windows Vista and Windows Server 2008" available at (www.microsoft.com/downloads/details.aspx?FamilyID=12ac9780-17b5-480c-aef7-5c0bde9060b0&displaylang=en), Published on March 2009.

[60] Nail Mansfield,"Practical TCP/IP: Designing, Using, and Troubleshooting TCP/IP Networks on LINUX and WINDOWS", ISBN: 0201750783, Addison-Wesley Publication 2003.Pages 27-82.

[61] Microsoft corp.," Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723)", Microsoft Security Bulletin MS09-048-Critical, 8th September 2009. available at (http://www.microsoft.com/technet/security/Bulletin/MS09-048.mspx)

[62] Microsoft corp., “How Windows firewall works” available at (http://technet.microsoft.com/en-us/library/cc755604.aspx), last access on: July-27, 2010.

[63] NETSCREEN-5GTUSER’S GUIDE, Version 5.0.0, Available at (http://www.juniper.net/techpubs/hardware/netscreen-appliances/netscreen-appliances50/ug_5gt.pdf), last access on: December-15, 2010.

[64] Inferring Internet Denial-of-Service Activity; available at (http://www.usenix.org/publications/library/proceedings/sec01/moore.html), last access on: July-27, 2010.

[65] Bob Rudis and Phil Kostenbader; “The enemy within: Firewalls and Backdoors” available at, (http://www.symantec.com/connect/articles/enemy-within-firewalls-and-backdoors), last access on: July-27, 2010.

[66] Avishai Wool, “A Quantitative Study of Firewall Configuration Errors”, IEEE Computer Society, vol. 37, no. 6, pp. 62-67, June 2004,

[67] Juniper Networks, Inc. “Attack detection and Defense Mechanisms” 2008 , is available online at (http://www.juniper.net/techpubs/software/screenos/screenos5x/ce_v4_5_0.pdf)

[68] Denial of Service and Attack Protection, available at (http://archive.cn.juniper.net/products/integrated/dos.pdf), last access on: July-27, 2010.

[69] Attack Detection and Prevention; Available at (http://www.juniper.net/techpubs/software/junos-security/junos-security10.0/junos-security-swconfig-security/id-68220.html#id-68220), last access on: July-27, 2010.

[70] Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide, available at (http://www.cisco.com/en/US/docs/security/asa/asa71/getting_started/asa5500/quick/guide/71GSG.pdf), last access on: December-15, 2010.

[71] Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman “Building Internet Firewalls” June 2000, Publisher: O'Reilly Media, Released: June 2000, Pages: 896.

[72] Defeating DDoS attacks; available at (http://www.ciscosystems.net/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/prod_white_paper0900aecd8011e927.html), last access on: July-27, 2010.

[73] Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks; available at (http://www.cisco.com/en/US/tech/tk59/technologies_white_paper09186a0080174a5b.shtml), last access on: July-27, 2010.

[74] DDoS Protection Solution Builds on Cisco Managed Service Leadership; available at (http://newsroom.cisco.com/dlls/2005/prod_060605b.html), last access on: July-27, 2010.

[75] Using CAR During DOS Attacks; available at (http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a00800fb50a.shtml), last access on: July-27, 2010.

[76] "Ascending the Managed Services Value Chain", Cisco Visual Networking Index Forecast, 2007-2012, June 2008; available at (http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns546/white_paper_c11-5540)

[77] Robert Richardson, "2008 CSI computer crime and security survey"; available at (http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf), last access on: July-27, 2010.

[78] Mafiaboy Pleads Guilty; avilable at (http://www.fbi.gov/pressrel/pressrel01/mafiaboy.htm), last access on: July-27, 2010.

[79] FBI ranks cyber attacks third most dangerous behind nuclear war and Weapons of Mass Destructions; available at (http://www.tgdaily.com/security-features/40861-fbi-ranks-cyber-attacks-third-most-dangerous-behind-nuclear-war-and-wmds), last access on: July-27, 2010.

## BIOGRAPHICAL SKETCH

Raja Sekhar Reddy Gade was born on April 27, 1987. He has done his Bachelors of Technology in Electronics and Communications from DPREC (JNT University), India on May 2008. He finished his Masters of Science in Electrical Engineering from The University of Texas-Pan American, Edinburg, Texas, US on December 20, 2010. He also served as teaching Assistant for Electrical Engineering department in UTPA from August 2008 to May 2010. He has also served as Research Assistant in the Networking Research Lab at UTPA.

His current mailing address is,

1809 West Schunior Street, Apt# 706,

Edinburg TX-78541.

Publications and Poster presentations during his Masters degree are,

[1] Raja Sekhar Reddy Gade, Hari V and S Kumar, "Performance of Windows XP, Windows Vista and Apple's Leopard Computers under a Denial of Service Attack," at (ICDS) International Conference on Digital Society on Feb 2010, publisher IEEE Computer Society.

[2] Raja Sekhar Reddy Gade, Sirisha. S, Hari. V and S. Kumar, "Impact of Land attack Compared for Windows XP, Vista and Apple's Leopard", Poster Presentation, HESTEC science symposium, Sep. 2009, at The University of Texas – Pan American.

[3] Raja Sekhar Reddy Gade, Sirisha. S, Leonel. A and S. Kumar , "Are Microsoft Windows Servers' capable of Defending against Security Attacks?" Poster Presentation, HESTEC science symposium, Nov. 2010, at The University of Texas – Pan American.

Publications under preparation during his Masters degree are,

[1] Raja Sekhar Reddy Gade, S Kumar, "Evaluation of Microsoft Windows Server 2003 and 2008 under TCP-SYN Denial of Service attack"

[2] Raja Sekhar Reddy Gade, S Kumar, "Performance of Juniper Networks Netscreen 5GT Firewall under common Denial of Service attack"