SYNOPSIS OF PH.D. THESIS ENTITLED

“PERFORMANCE EVALUATION AND OPTIMIZATION FOR DISTRIBUTED NETWORK FIREWALL DESIGN”

SUBMITTED TO
KADI SARVA VISHWAVIDYALAYA,
GANDHINAGAR, GUJARAT, INDIA

FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY (PH.D.)

IN
ELECTRONICS & COMMUNICATION

BY

CHIRAG LALITBHAI SHETH
(REGISTRATION NO. 10D0293)

UNDER THE SUPERVISION OF
DR. RAJESH THAKKER
PROFESSOR AND HEAD
ELECTRONICS & COMM. DEPTT.,
VISHWAKARMA GOVT. ENGG. COLLEGE, CHANDKHEDA, 382424
(FEB, 2016)
SYNOPSIS OF PH.D. THESIS ENTITLED

“PERFORMANCE EVALUATION AND OPTIMIZATION FOR DISTRIBUTED NETWORK FIREWALL DESIGN”

SUBMITTED TO : KADI SARVA VISHWAVIDYALAYA, GANDHINAGAR, GUJARAT, INDIA.

FACULTY : ENGINEERING & TECHNOLOGY

SUBJECT : ELECTRONICS & COMMUNICATION

RESEARCH STUDENT : CHIRAG SHETH

RESEARCH GUIDE : DR. RAJESH THAKKER

REGISTRATION NO. : 10D0293

DATE OF REGISTRATION : 25/09/2010

(DR. RAJESH THAKKER) (CHIRAG SHETH)
RESEARCH SUPERVISOR RESEARCH STUDENT
1. Introduction

Network Firewalls protect a trusted network from an untrusted network by filtering traffic according to a specified security policy. A firewall is often placed at the entrance of each private network in the Internet. The function of a firewall is to examine each packet that passes through the entrance and decide whether to accept the packet and allow it to proceed or to discard it. A firewall is usually designed as a sequence of rules. Although the subject is highly discussed during recent times, not much practical research has been done on this topic.

Significant work on network firewalls has been carried out by M. G. Gouda and A. X. Liu by proposing structured firewall design [1] and by H. Hamed, et al. on firewall packet filtering mechanisms [2, 3]. Notable work have also been done on Distributed Denial of Service (DDoS) attacks detection model and defense [4 - 8]. However, not much importance has been laid on analyzing network firewall performance during DDoS attack. Muhammad et al. also made notable contribution by carrying out analysis of firewall policy rules using traffic mining techniques [9]. H. Acharya and M. Gouda came up with linear-space verification of firewall policy [10]. Qi Duan and Ehab Al-Shaer also carried out significant work in classification of traffic-aware dynamic firewall policy management and techniques [11]. However, most work has shortfall of practical implementations. Notable work have also been done on firewall security enhancements and next generation firewalls [12 - 15].

This research work attempts to focus on the same and try to evaluate performance of firewall technology. Approach is suggested to improve performance of distributed firewall design. Initially, a structured method for testing firewall performance is proposed by evaluating and comparing performance of major firewalls in operation today. Detailed analysis and comparison is done in terms of cost, security, operational ease and implementation of Open source packet filter (PF) firewall, Checkpoint SPLAT and Cisco ASA in a testing environment with laboratory generated traffic in closed environment. Since firewall needs to show robust performance along with application intelligence in order to withstand against Distributed Denial of Service (DDoS) attack, firewall performance during DDoS attack is studied and methods to improve performance is proposed.

With the growth of network complexity, it is very common to find firewall policies with thousands of rules. Modern firewall rulebase are growing in size and complexity at an exponential rate. As changes add up, the firewall rule base gets more complex. Firewall rulebase works on first-match principle. As a result, there exists scope of improvement in firewall performance, if highest utilized rule is brought ahead in rulebase. This will facilitate earlier matching and hence less firewall resource utilization. This is carried out carefully without compromising overall firewall security or without
loss of semantic integrity through a framework for rulebase reordering based on traffic conditions. To evaluate the performance of approach, performance testing on OpenBSD PF firewall is carried out by reordering rulebase under closed environment.

Further, system and method comprising standalone network design for interconnection of firewalls at multiple geographical locations connected through wide area Open Source network is proposed in order to improve scalability and security. This will overcome limitation and traditional bottleneck of static site to site Virtual Private Network (VPN). To evaluate the performance of the approach and proposed design, OpenBSD PF firewall performance testing is carried out under laboratory setup.

2. Problem Definition

(1) In spite of exponential rise in firewall deployment, no standard method of firewall performance evaluation is prevalent in market. The primary reason for the same is that firewall implementations vary widely making it difficult to carry out direct performance comparisons. As more and more organizations deploy firewalls on their networks, question arises whether the products will stand up to and sustain to relatively heavy loads. Today, increasing attention is paid to firewall rule-set quality due to regulations such as the Sarbanes-Oxley act [SOX02] and the CobiT framework [Cob08]; the Payment-Card Industry Data Security Standard (PCI DSS) [PCI06]; and the NIST standard 800-41 [NIS02]. All these regulations include specific sections dealing with firewall configuration, management, and audit.

(2) Distributed denial-of-service (DDoS) attacks are a major threat to the Internet. Network firewalls act as the first line of defense against unwanted and malicious traffic and also represent critical point of failure during DDoS attack. Predicting the overall firewall performance is crucial to network security administrators and designers in assessing the strength and effectiveness of network firewalls against DDoS attacks. Good amount of research is being undertaken to detect, prevent, delay and trace back DDoS attacks. Most of researchers and network administrators are doing post attack forensics which comes after the attack has taken place. Firewall deployments are critical considering magnitude and volume of DDoS attacks. Most of the companies are paying large amount of money on annual basis to buy specialized DDoS mitigation and protection gear to protect their web applications during DDoS attack, which they may never use it. Also, most network providers and managed services hosting providers have no real operational solution to stop DDoS attacks. Hence the firewall needs to show robust performance along with application intelligence in order to withstand against DDoS attack.

(3) Once a firewall is acquired, a firewall administrator has to configure and manage it to realize an appropriate security policy for the particular needs of the company. The single most important factor of firewall's security is how it is configured. It is generally accepted among network security experts that corporate firewalls are poorly
configured. Today, it is very common to find firewall policies with thousands of rules, making firewall rulebase complex. With the increase in size of firewall rulebase, packets have to traverse more number of rules in order to arrive at matching conditions. With lots of promiscuous, redundant, orphaned and shadowed rules in the rulebase, optimal reordering of rulebase is needed in order to improve firewall performance.

(4) Today, with growth and expansion, most companies are geographically spread all over the world. There is a need for increased network security when connecting inside protected networks spread in different geographical location, specifically over internet. One of the known approach to avoid sending data in plain text over internet is to establish site to site virtual private network (VPN) using firewall at both locations. VPN will ensure data security by encrypting the traffic. However, major challenge with site to site VPN is that it provides static network routing. In case of multiple sites, each site needs dedicated site to site VPN connectivity with all other sites. This increases network complexity and bottleneck in case of any site or link failure.

3. Objective and Scope of work

The objective of the thesis is to improve and optimize Network Firewall performance. Since, no standard method for testing firewall performance is available, initial objective is to establish a testing mechanism to measure firewall performance. Further, objective is to identify and improve the key performance parameters of firewall. Some of the firewall performance parameters identified for improvement as a part of this thesis are – Throughput (TCP, HTTP, and UDP), CPU Utilization, Concurrent Connections, performance during DDoS, scalability and security. Firewall performance improvement by rulebase re-ordering according to traffic pattern is worked upon. Further, optimized and scalable design for interconnection of multiple firewalls through a standalone open source network is proposed.

4. Thesis Contributions

- Most currently undertaken and reported research work on firewall have been carried out theoretically and lacks practical implementation. Attempt has been made by undertaking work to compare performance of various firewalls based on practical implementation. Comparison of various firewalls presented in this research will also help in selecting right vendor at time of firewall procurement.
- The study will help researchers gain a good understanding of existing work on rulebase optimization, and framework presented could help firewall administrators to be aware of this important problem and adopt an approach to optimize their own network firewall performance.
- Test results will help in identifying pre-deployment capacity planning and testing network performance to ensure that the increased security does not degrade performance beyond the levels acceptable for the business.
- Today, DDoS attacks are major threat to internet security and most network service providers have no real
operational solution to stop it. Work carried out highlights firewall DDoS performance parameters and also suggested approach to minimize impact of DDoS.

- Method proposed for firewall rulebase reordering based on traffic logs will help improving firewall throughput and hence, decrease overall network latency.
- Cost effective and optimized design of interconnection of firewalls at multiple locations through standalone network will provide an alternate approach for Network administrators to make their network scalable with Open source solution.

5. Firewall Performance Testing setup and results

Major types of firewalls operational as on today are examined. Detailed analysis and comparison is done in terms of performance, security, operational ease and implementation of Open source packet filter (PF) firewall, Checkpoint SPLAT and Cisco ASA in a testing environment with laboratory generated traffic in closed environment.

A. Laboratory Setup

In order to characterize performance of firewall, the testing environment setup shown in Fig. 1 is used to compare performance of three most operational firewalls in market.

![Fig. 1 - Setup diagram for performance testing.](image)

Test traffic is generated using Open-Source tool called Curl-Loader. The Curl-Loader is capable of simulating application behavior of hundreds of thousands of http/https clients, each with its own source IP-address. Performance of System under Test (SUT) is tested with necessary laboratory traffic generated with gateway in the middle and under various scenarios.
Table I provides configuration details of firewalls used for testing.

<table>
<thead>
<tr>
<th>Firewall Configurations</th>
<th>System Under Test – Firewall Products</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco ASA</td>
</tr>
<tr>
<td>Platform</td>
<td>Cisco ASA – 5580</td>
</tr>
<tr>
<td>Operating System</td>
<td>ASA V 8.2.2</td>
</tr>
<tr>
<td>Product Architecture</td>
<td>Multi-processor, Multi-core</td>
</tr>
<tr>
<td>Processing Cores</td>
<td>8</td>
</tr>
<tr>
<td>Gigabit Ethernet Interfaces</td>
<td>0</td>
</tr>
<tr>
<td>10 Gigabit Ethernet Interfaces</td>
<td>4</td>
</tr>
</tbody>
</table>

B. Performance Testing Results
Some of the major Key Performance Indicators (KPI) given in Table II are explored in order to compare performance of firewall products used for testing.

<table>
<thead>
<tr>
<th>Key Performance Indicators (KPI)</th>
<th>System Under Test – Firewall Products</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco ASA</td>
</tr>
<tr>
<td>Firewall Licensing</td>
<td>Proprietary</td>
</tr>
<tr>
<td>Application Intelligence</td>
<td>Yes</td>
</tr>
<tr>
<td>Firewall Management</td>
<td>Local</td>
</tr>
<tr>
<td>HTTP Throughput (Gbps)</td>
<td>10.6</td>
</tr>
<tr>
<td>TCP Throughput (Gbps) (Object size = 512 KB)</td>
<td>18.6</td>
</tr>
<tr>
<td>Concurrent Connections</td>
<td>200K</td>
</tr>
<tr>
<td>UDP Throughput (Gbps) (Object size = 512 KB)</td>
<td>8</td>
</tr>
<tr>
<td>Connections per Second</td>
<td>160K</td>
</tr>
</tbody>
</table>

Fig. 2 - Throughput and connections comparison.
C. Observations and Deviation from Data Sheets
For the configuration used in testing setup, Cisco mentions of achieving up to 10 Gbps of real-world HTTP firewall throughput performance and 1,50,000 connections per second. The results shown in Fig. 2 agree with the same. In fact, we are able to achieve 10.2 Gbps HTTP throughput with real world traffic and around 160,000 connections per second. It is slightly better compared to performance reported by Cisco. In comparison, Checkpoint mentions of achieving up to 12 Gbps of maximum HTTP throughput performance. However, Checkpoint recommends IBM systems for achieving maximum throughput, and also mentions that throughput performance may vary depending on hardware. In testing setup, 5.6 Gbps throughput is achieved with HP Hardware Platform. OpenBSD also mentions that performance of PF firewall varies with hardware platform, performance of system bus, efficiency of network card and type of application. PF is a kernel-based process and therefore, it will not use swap spare and will degrade in performance with lesser RAM size. In laboratory setup, 4.5 Gbps HTTP throughput performances with HP hardware platform is achieved. The performance testing results indicates that Cisco ASA provides better performance and Checkpoint SPLAT provides better functionality. OpenBSD PF also proves to be best open source solution if cost is the deciding factor. Checkpoint provides better Firewall Management with centralized policy management and better user interface than Cisco and PF.

Choosing the right firewall depends on the needs of business and network. Cisco ASA is one of the best choices for large corporate networks. For complex production networks which demand high protection, Checkpoint SPLAT provides an upper edge over Cisco. PF is one of the best inexpensive open source solutions which provides equally competent performance as compared with proprietary products, but lacks on application layer intelligence.

6. Firewall DDOS Performance Testing and Improvement

In order to characterize performance of firewall, the testing environment setup shown in Fig. 3 is used to compare performance of three most operational firewalls in market. The traffic is targeted towards a web application hosted on web application servers at the other side. The firewall policy is set to allow all the requests on port http and https towards the targeted IP where web services are hosted, hence firewall job is to establish state and forward the packet. Packets and states are observed on the firewall using various tools and CLI commands. The configurations, operating system and hardware details of three firewall products under test are as mentioned in TABLE I with OS upgrades. Cisco uses its own hardware and Checkpoint and PF are configured on HP Servers. We tried to keep hardware as similar as possible for all three firewalls under test.
A. Performance Testing Results

The performance testing results in Table III indicates that no firewall proved to be capable of withstanding DDoS for longer time. As the intensity of DDoS increases, Checkpoint showed higher initial resistance and allowance of legitimate traffic compared with other two. However, CPU utilization of Checkpoint is higher as compared with Cisco ASA and PF Firewalls. Time before all three firewall becomes unreachable is very less even to react to DDOS. It appears that although the firewalls are stateful, during DDoS attack, each set of packets traversing a stateful firewall consumes state-table resources within those firewalls, creating a DDoS chokepoint. Hence at high intensity DDoS state tables resources of all three firewalls get consumed making them unreachable in short time. All three of them gave priority to TCP traffic than ping and UDP during DDOS.

<table>
<thead>
<tr>
<th>DDoS Performance Parameters</th>
<th>System Under Test – Firewall Products</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco ASA</td>
</tr>
<tr>
<td>HTTP Throughput (Gbps)</td>
<td>10.6</td>
</tr>
<tr>
<td>Legitimate Traffic allowed till % of DDOS traffic</td>
<td>80%</td>
</tr>
<tr>
<td>Firewall CPU Utilization at 50% DDOS</td>
<td>40%</td>
</tr>
<tr>
<td>Firewall CPU Utilization at 75% DDOS</td>
<td>60%</td>
</tr>
<tr>
<td>Time for complete failure (unreachable) at full DDOS</td>
<td>12 min</td>
</tr>
<tr>
<td>Capacity limits (% of other traffic blocked except TCP)</td>
<td>100%</td>
</tr>
</tbody>
</table>
After analyzing firewall performance during DDoS attack, performance improvement is achieved by varying some of the parameters and by controlling state table entries.

**B. Performance Improvement by tweaking TCP Opening Timer during SYN Flood Attack**

Experiments are carried out by tweaking TCP.opening timer value from default 30 sec to 1 sec. Testing is carried out in same setup as used earlier. OpenBSD PF firewall is chosen considering it being open source and flexibility to change parameters from source code. Different intensity of laboratory generated traffic is used to test performance. CPU Utilization is taken as key performance indicator along with firewall state table with half closed states. The results obtained shows consistent improvement in CPU utilization of firewall hardware when we set the TCP.opening value as 1 second during SYN flood attack in which only SYN packets are send for denial of service. Changing TCP.opening value to 1 second might pose disadvantage that firewall will not keep states more than 1 sec for established connection. However during DDoS, lowering this value proves to be helpful in improving firewall performance.

### TABLE IV
TEST RESULTS BY TWEAKING TCP TIMER IN OPENBSD PF FIREWALL

<table>
<thead>
<tr>
<th>Laboratory Traffic generated HTTP conn./sec</th>
<th>Tcp.opening = 30 s</th>
<th>Tcp.opening = 1 s</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No. of half-closed States</td>
<td>CPU Utilization</td>
</tr>
<tr>
<td>5 K</td>
<td>145 K</td>
<td>25%</td>
</tr>
<tr>
<td>50 K</td>
<td>1.3 M</td>
<td>59%</td>
</tr>
<tr>
<td>100 K</td>
<td>2.1 M</td>
<td>89%</td>
</tr>
</tbody>
</table>

Results indicate that lowering the value of TCP timers for stateful firewalls help improving firewall performance during DDoS attack. In any setup, optimal value of timer should be chosen after taking into consideration web application and network environment.

**C. Performance Improvement by DDoS Identification and Mitigation by controlling states in Firewall State Table**

Most of the firewalls used today are stateful inspection firewalls. They perform the same function as packet filter firewalls, but with the ability to keep track of the state of connections in addition to the packet filtering abilities. By dynamically keeping track of whether a session is being initiated, currently transmitting data (in either direction), or being closed, the firewall can apply stronger security to the transmission of data. A stateful inspection firewall is capable of understanding the opening, communication, and closing of sessions. Stateful inspection firewalls usually have a fail-close default configuration, meaning that they will not allow a packet to pass if they do not know how to handle the
packet. Overall, stateful inspection firewalls give high performance and provide more security features than packet filtering. Such features can provide extra control of common and popular services. Stateful inspection firewalls support most (if not all) services transparently, just like packet filters, and there is no need to modify client configurations or add any extra software for them to work. However, during DDoS attack, keeping state table entries results in exhaustion of firewall state table and not able to accept any more states.

Intelligence is induced in firewall to identify hosts which are source of DDoS. Code introduced in OpenBSD PF Firewall to only keep states in the firewall state table which satisfy specified conditions. Maximum state in the state table is set to 2 million. Once it reaches, it starts discarding older state table entries. Also, particular host can have maximum of 10000 concurrent connections or state table entries. This will ensure protection against DoS attacks. Apart from that source connection rate is kept as 1000 connections per 10 seconds. If any host is making requests faster, then it will be discarded and state table will be cleaned up. Also all such hosts who will meet this criterion will be further blocked and entries for that host will be discarded. The maximum limits set are optimal for laboratory setup and has proved to be effective in mitigating laboratory generated DDoS in setup used.

7. Proposed Framework for Dynamic Firewall Rulebase Restructuring based on traffic to improve performance

In order to improve firewall performance, framework is proposed to arrive at optimal restructuring of rulebase based on traffic conditions.

A high level block diagram of proposed algorithm is presented in Fig. 4. Various components / blocks are as explained as follows -

![Diagram](image)

Fig. 4 - Framework for Firewall rulebase reordering based on traffic conditions

The firewall logs its actions by writing records to a log file. Each record in the log file corresponds to a single connection that the firewall filtered. The log record contains many fields, such as – time stamp, rule identifier, source, destination, ports, protocol, state details, packet details etc. The firewall log file is analyzed to get information on rules utilization and corresponding traffic distribution is obtained by capturing log files for particular duration. Rule usage value is
between 0 and 1 and it gives relative indication on frequency of usage of particular rule. A rulebase of R firewall rules therefore comprises of R rules, each associated with R usage frequencies which will have value between 0 and 1.

Rule Usage Figure = \( F_1 \) (Corresponding to Rule 1), \( F_2 \) (Corresponding to Rule 2)... \( F_R \) (Corresponding to Rule R).

Based on individual rule usage, overall rulebase weight is calculated which is summation of all individual rule usage.

Rulebase Weight for particular rule ordering = Summation of individual rule usage = \( \sum_{x=1}^{R} x \ast F_x \)

This Rulebase Weight is calculated for particular order of firewall rulebase and it will be unique for that order. Successive rules will be swapped repeatedly based on Rule Usage and new Rules Weight will be calculated. If its value is lower than earlier, then rules will be swapped. This will be repeated till no further swapping of rules is needed.

Firewall Rule SAFETY: Changing the order of rules in a rulebase may result in firewall prone to security threats if not done properly. Moving a rule to an earlier location in the rule base, without maintaining safety, can easily change the action that is applied to certain IP connections which will further cause security breaching. A rule movement is considered to maintain semantic integrity, if the reordered rule-base causes the firewall to make exactly the same filtering actions as it did before re-ordering. It is most important to restructure firewall policies based on traffic conditions, without losing semantic integrity.

Performance Testing Setup and Results

Implementation is carried out of the discussed framework on OpenBSD Packet Filter (PF) Firewall in order to measure performance improvement. In order to characterize performance of firewall, the testing environment setup shown in Fig. 5 is used. The firewall configurations, operating system and hardware details of OpenBSD firewall under test are mentioned in Table V.

Experimental setup is carried out on OpenBSD PF Firewall which consisted of 286 rules in the rulebase. This is comparable to a medium to small sized network firewall. Initially, entire rulebase is divided into blocks based on
network filtering actions and then, rules are re-ordered based on their usage as per proposed algorithm.

### TABLE V

**SYSTEM UNDER TEST (FIREWALL) CONFIGURATIONS**

<table>
<thead>
<tr>
<th>Configurations</th>
<th>OpenBSD PF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Platform</td>
<td>HP DL 380</td>
</tr>
<tr>
<td>Operating System</td>
<td>Open BSD 4.7</td>
</tr>
<tr>
<td>Product Architecture</td>
<td>Multi-processor, Multi-core</td>
</tr>
<tr>
<td>Processing Cores</td>
<td>8</td>
</tr>
<tr>
<td>Gigabit Ethernet Interfaces</td>
<td>0</td>
</tr>
<tr>
<td>10 Gigabit Ethernet Interfaces</td>
<td>4</td>
</tr>
</tbody>
</table>

Traffic is captured through TCP dump utility. Fig. 6 shows traffic distribution for the 284 rules in the rulebase. Rule Usage and further initial Rulebase Weight is calculated based on this distribution values.

![Traffic Distribution](image)

**Fig. 6 - Initial Traffic Distribution**

Algorithm for firewall rulebase reordering based on traffic conditions is applied and rules are successively swapped to arrive at re-ordered optimized ruleset. Further, testing is carried out to study impact on firewall performance as mentioned in Table VI. Similar laboratory traffic is applied to same firewall under test before and after re-ordering of rulebase in order to compare performance. TCP throughput and concurrent connections are the key performance indicators considered.

### TABLE VI

**PERFORMANCE TESTING RESULTS**

<table>
<thead>
<tr>
<th>Key Performance Indicators (KPI)</th>
<th>System Under Test – OpenBSD PF Firewall</th>
<th>Performance Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Throughput (Gbps) (Object size = 512 KB)</td>
<td>Pre Rulebase Reordering: 9.4 Gbps, Post Rulebase Reordering: 10.3 Gbps</td>
<td>9.57%</td>
</tr>
<tr>
<td>Concurrent Connections</td>
<td>Pre Rulebase Reordering: 420K, Post Rulebase Reordering: 500K</td>
<td>11.9%</td>
</tr>
</tbody>
</table>
8. Scalable Design of Open Source based Dynamic Routed Network for Interconnection of Firewalls at Multiple Geographic Locations

In order to improve scalability with improved security and mitigating risk of site to site connectivity of traditional site to site Virtual Private Network (VPN), design is proposed for interconnection of firewalls at multiple geographic locations through Open Source network. The proposed network design is for global or wide area network that interconnects all sites at different geographical location and also interconnects all the networks within the same site.

![Diagram of multiple sites layout]

**Fig. 7 - Multiple sites Layout.**

In the proposed setup mentioned in Fig. 7, a standard firewall has the following setup -

1. Internet interface for connecting to internet.
2. Interface for connecting to routing device of proposed network.
3. Inside interface(s) for connecting to protected network.

The standalone network consists of the device used for routing and the links connecting them. For inter-site connectivity the links between routing devices is proposed to use internet protocol security (IPsec) captured generic routing encapsulation (GRE) tunnels. Within a site, it is proposed to be direct links or VLAN sub-interfaces. Inter-site traffic is always encrypted, no matter if the carrier is the internet or a dedicated data service. Inside the proposed network, there is no filtering of traffic. It is a dynamically routed network that uses Border Gateway Protocol (BGP) for routing. Also, the
network is split up into multiple autonomous systems (AS) to stabilize the routing. Stabilization of traffic will help preventing BGP breakdown. The design uses one backbone AS and multiple leaf AS. The leaf AS connects the backbone AS for connectivity to the rest of the network.

A. Performance Measurement of OpenBSD Firewall

Tests are carried out to measure performance of OpenBSD Firewalls in the proposed design. Two sites are used and the description of the tests is as follows –

(1) Raw packets per second (pps) Test

The testing setup for raw pps test is as follows –

- OpenBSD PF Firewall at each site, running two VLANS with rulebase having two sections of rules for each vlan network.
- OpenBSD Routing Devices at each site, used to forward packets.
- Target Servers running Netcat socket
- Generator Servers running Netcat over TCP (use of dd command)
- MTU on Generator Server = 256 bytes.

Configurations of all the systems used for testing are mentioned in Table VII.

<table>
<thead>
<tr>
<th>Configurations</th>
<th>OpenBSD PF &amp; Routing Device</th>
<th>Generator Server</th>
<th>Target Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Platform</td>
<td>Supermicro X9SRD-F</td>
<td>Supermicro X9SRD-F</td>
<td>Supermicro X9SRD-F</td>
</tr>
<tr>
<td>Operating System</td>
<td>Open BSD 5.5</td>
<td>Kali Linux</td>
<td>Kali Linux</td>
</tr>
<tr>
<td>Product Architecture</td>
<td>Multi-processor, Multi-core</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processing Cores</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Netcat is used considering it opens an encryption-less connection from one host to another. “dd” command is used for writing raw data blocks from one place to another. Since it can read directly from raw device files, it is very useful for copying entire partitions or drives from one location to another. The test is successful, and it is observed that firewalls are processing 600kpps of traffic and running stable for a long time.

(2) HTTP packets per second (pps) Test

The http pps test is carried out with the same setup as used for raw pps test, except it uses AB (ApacheBench) and NGNX for generating and receiving the traffic. AB is a single-threaded, command line computer program which loads the test servers by sending an arbitrary number of concurrent requests. Nginx is an open-source, high-performance HTTP server.
The testing setup for HTTP pps test is as follows –

- OpenBSD PF Firewall at each site, running two VLANS with rulebase having two sections of rules for each vlan-network.
- OpenBSD Routing Devices at each site, used to forward packets.
- Target Servers running Nginx
- Generator Servers running AB
- MTU on all servers 256 bytes

The test is successful and generated http traffic to and from the VLANs. In the laboratory setup described, OpenBSD PF firewall processes 360kpps with about 80% CPU load.

## B. High Capacity Site Design

A standard site contains routing device which connects all the firewall edge devices and other routing devices. It also connect to other sites using IPsec encapsulated GRE tunnels. At backbone sites the routing devices also need to process traffic between remote sites. The IPsec processing is a lot more CPU intensive than just forwarding. When the device needs to handle IPsec traffic, local forwarding performance is greatly reduced. To increase the capacity of the site, a site routing device is proposed. This device is dedicated to routing traffic inside a site. It takes over the task of interconnecting all the network core and edge devices at a site from the routing device. With this site routing device in topology, the routing devices are no longer need to process traffic between local devices, they only need to handle VPN traffic. As a result, VPN capacity will be increased by adding additional routing devices to the site. The new devices will take care of the routing between all devices.

A typical setup has site routing devices usually in pairs for high availability is shown in Fig. 8.

---

Fig. 8 - Design Layout with Site and Interconnect routing devices.
C. Performance Tests for High Capacity Site Design

Tests are carried out to measure forwarding performance with different packet sizes. A single site router with two edge interfaces and one core interface is used for testing. Two Gigabit Ethernet interfaces are configured as a failover trunk, with VLAN-interfaces configured on the trunk. MTU are configured on generator and receiver interface to test with different packet sizes. Systems configuration are similar to that used during Raw Packets per Second (pps) test above as per TABLE VII.

In the laboratory setup, results are obtained by changing MTU in order to test forwarding performance with different packet sizes.

<table>
<thead>
<tr>
<th>Maximum transmission unit (MTU)</th>
<th>CPU Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU 128 byte</td>
<td>98.6%</td>
</tr>
<tr>
<td>MTU 256 bytes</td>
<td>95.9%</td>
</tr>
<tr>
<td>MTU 512 bytes</td>
<td>95.5%</td>
</tr>
<tr>
<td>MTU 1024 bytes</td>
<td>79.7%</td>
</tr>
<tr>
<td>MTU 1434 bytes</td>
<td>69.6%</td>
</tr>
</tbody>
</table>

The tests indicates that as MTU increases, CPU utilization decreases. Since protocol overheads remains constant, larger MTU will be able to carry more data. As a result, CPU utilization decreases with increase in MTU size. It is also observed that CPU utilization falls more sharply for MTU larger than 512 bytes. No packet drop is observed which reflects the correctness of proposed design. It is also observed that OpenBSD site router is capable to handle 380kpps with MTU of 256 bytes before it is fully utilized, which gives us around 700Mbps of bandwidth. Hence, under standard size MTU (256 bytes), it is recommended to use OpenBSD Site router setup if it is required to move up to 700 Mbps of traffic. Results obtained are limited to laboratory environment under discussion and it may vary depending on actual network environment and traffic conditions.
9. Conclusion

Initial literature review indicated that standard method for testing firewall performance does not exist. As a result, attempt was made to propose a structured method for testing firewall performance. Further, evaluation of performance of major operational firewalls in market is carried out along with comparative analysis. Firewalls like Cisco ASA, Checkpoint SPLAT and OpenBSD PF are compared against key performance indices identified as Throughput (HTTP, TCP, and UDP), connections per second, concurrent connections, licensing and application intelligence. Results obtained were compared with datasheets provided by proprietary firewalls and deviations are highlighted. Further, security testing results indicated that all the three firewall demonstrated basic intrusion detection capability and blocked transmission against common attack types.

Further, analysis of firewall performance during DDoS attack is carried out. Most currently undertaken and reported research work on DDoS focus on other parameters, and firewall performance is not given due importance. The suite of tests are performed to help determine the performance and behavior of the firewall under various levels of DDoS attacks. The performance testing results indicated that no firewall proved to be capable of withstanding DDoS for longer time. Checkpoint showed higher initial resistance and allowance of legitimate traffic as intensity of DDoS increases as compared with Cisco and PF. However, CPU utilization of Checkpoint is higher as compared with Cisco ASA and PF firewalls. Time before all three firewall becomes unreachable is very less even to react to DDoS. At high intensity DDoS state tables resources of all three firewalls get fully consumed making them unreachable in short time. Experiments are performed to show improvement in firewall performance by tweaking TCP Opening timer during SYN Flood attack. Various parameters are changed in order to control state table entries to mitigate DDoS attack and attempt is made to introduce intelligence in firewall to successfully mitigate DDoS in closed laboratory environment.

Growth in network increases complexity in firewall rulebase. It is important that it should not impact firewall performance. To the best of available literature, most currently undertaken and reported research work on firewall rulebase optimization is theoretical and lacks practical implementation. Classification of firewall rulebase optimization methods is carried out with focus on rulebase reordering based on traffic conditions. Framework is proposed to arrive at optimal reordering of rulebase based on traffic conditions. This is carried out by analysis of firewall logs during finite interval of time. Reordering of rules is carried out within blocks and by maintaining semantic integrity and firewall safety. Performance testing with laboratory traffic is carried out on OpenBSD PF firewall. It is observed that after firewall rulebase reordering, there is performance improvement in firewall throughput by 9.57% and improvement in concurrent sessions supported by firewall by 11.9%.

Further, to improve scalability and security, system is proposed comprising Open source network for interconnection of firewalls at multiple geographical locations connected through wide area network and also interconnection of all the
networks within the same site. It applies to all communication to internal networks that is not behind the local firewall. Performance tests carried out on PF firewalls in the proposed setup confirms that firewalls are processing 600kpps of traffic under raw pps test and 360kpps of HTTP traffic with about 80% CPU load on the OpenBSD Firewall. Network design for sites which needs higher capacity as compared with other network sites is also proposed. Performance tests of the setup is carried out under laboratory traffic and it is inferred to use Site router setup if it is required to support up to 700 Mbps of traffic.

10. Future Work

Work carried out is limited to Firewall products from Cisco, Checkpoint and OpenBSD PF. Work could further be extended by using products from other firewall vendors for comparative analysis. Also, HP and Supermicro hardware were used during setups. Firewall performance will vary with different make and model of hardware, performance of system bus and efficiency of network interfaces. Word carried out could be extended by using other make and model of hardware. Re-ordering of firewall rulebase based on traffic logs could be further extended by creating automated scripts and setup scheduled task which runs the script daily / weekly and rearranges the rules based on traffic logs. To study the impact of firewall rulebase reordering, firewall with 284 rules was taken. This could further be extended by taking complex firewalls with large number of rules, as this will pose the challenge of maintaining semantic integrity of rules.

11. List of Publications


12. Patent Filed

Indian Patent filed on “SYSTEM AND METHOD FOR INTERCONNECTION OF FIREWALLS AT MULTIPLE GEOGRAPHIC LOCATIONS THROUGH A STANDALONE NETWORK”

Patent has been filed at MUMBAI PATENT OFFICE with below details -

Reference: CBR No. 1740

Patent no. 384/MUM/2015

Date of filing: 05th Feb 2015 11:59:11

13. IETF Submission

IETF Draft titled “Dynamic Routed Network for Interconnection of Firewalls at Multiple Geographic Locations” has been submitted on 10th Nov 2015.

14. References


(9) Muhammad Abedin, Syeda Nessa, Latifur Khan, Ehab Al-Shaer, Mamoun Awad, “Analysis of firewall


Also, some of the Request for Comments (RFC) on TCP and firewalls studied are as below -


RFC 5482 - TCP User Timeout Option.

RFC 6298 Computing TCP’s Retransmission Timer.

RFC 4732 - Internet Denial-of-Service Considerations.

RFC 2647 - Benchmarking Terminology for Firewall Performance.

RFC 3511 - Benchmarking Methodology for Firewall Performance.

RFC 2979 - Behavior of and Requirements for Internet Firewalls.