::jseblod::article_c::/jseblod::
::photo_x::6::/photo_x::

::jseblod_photo_x::photo_x::/jseblod_photo_x::
::article_basic_layout|0|photo_x::Left::/article_basic_layout|0|photo_x::
::article_text|0|photo_x::**"Cyber Attacks Hit 75% of Global Enterprises in 2009"** [Symantec, Feb-2010]
"IT Security spending to outpace other IT spending in 2010" [Gartner Research, Dec 2009]

Today, increasing attention is paid to firewall rule-set quality due to regulations such as the Sarbanes-Oxley act, CobiT framework, the Payment-Card Industry Data Security Standard (PCI DSS) and the NIST standard 800-41. All these regulations include specific sections dealing with firewall configuration, management and audit.

The document will begin with current analysis of Vulnerabilities in Internet Firewalls. Various types of firewalls which are operational today will be examined and cross reference each firewall operation with causes and effects of weaknesses in that operation, analyzing reported problems with available firewalls. Detailed analysis and comparison will be done in terms of cost, security, operational ease and implementation of Open source packet filter (PF) firewall, Checkpoint SPLAT and Cisco PIX.

Various policy anomalies in Distributed firewalls will be studied to make firewall scalable. Packet filtering mechanisms in various firewalls will be studied and comparative analysis will be done. Various common configuration errors in installation/management of network firewall will be studied and summarized. Conclusion will be made to design a structured method for configuring firewall rulebase to be correct, consistent, complete, and compact.

::/article_text|0|photo_x::
::photo|0|photo_x::images/photos/1594/Firewall-HTE.jpg::/photo|0|photo_x::
::photo_size|0|photo_x::Quarter::/photo_size|0|photo_x::
::ad_unit|0|photo_x:: ::/ad_unit|0|photo_x::
::jseblodend_photo_x::::/jseblodend_photo_x::
::jseblod_photo_x::photo_x::/jseblod_photo_x::
::article_basic_layout|1|photo_x::Left::/article_basic_layout|1|photo_x::
::article_text|1|photo_x::**Introduction**

Network Firewalls protect a trusted network from an un-trusted 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 the packet. A firewall is usually designed as a sequence of rules. A firewall's basic task is to regulate some of the flow of traffic between computer networks of different trust levels. Typical examples are the Internet which is a zone with no trust and an internal network which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter network" or Demilitarized zone

(DMZ).

A firewall's configuration contains a large set of access control rules, each specifying source addresses, destination addresses, source ports, destination ports, one or multiple protocol ids, and an appropriate action. The action is typically "accept" or "deny." Some firewalls can support other types of actions such as sending a log message, applying a proxy, and passing the matched packets into a VPN tunnel. For most firewalls, the rule set is order-sensitive. An incoming packet will be checked against the ordered list of rules. The rule that matches first decides how to process the packet. Due to the multidimensional nature of the rules (including source/destination addresses and ports), the performance of a firewall degrades as the number of rules increases. Commercially deployed firewalls often carry tens of thousands of rules, creating performance bottlenecks in the network. More importantly, the empirical fact shows that the number of configuration errors on a firewall increases sharply in the size of the rule set. A complex rule set can easily lead to mistakes and mal-configuration.

Despite their critical role, firewalls have traditionally been tested without well-defined and effective methodologies. Currently, a diverse set of firewalls is being used. Because it is infeasible to examine each firewall separately for all potential problems, a general mechanism is required to understand firewall vulnerabilities in the context of firewall operations. The firewall data flow model we presented gives an overall description of firewalls by detailing the operations they perform (depicted in figure 1). When a packet is received by a firewall, it first undergoes link layer filtering. Then it is checked against a dynamic rule set. The packet then undergoes packet legality checks and IP and port filtering. Finally, network/port address translation is performed. Sophisticated firewalls also reassemble packets and perform application level analysis. After a routing decision is made on the packet, out-bound filtering may also be performed. Each of these operations is optional, and the order in which the packet traverses them may also differ in different firewalls.::/article_text|1|photo_x::
::photo|1|photo_x::::/photo|1|photo_x::
::photo_size|1|photo_x::Full::/photo_size|1|photo_x::
::ad_unit|1|photo_x::Medium_Rectangle_All_300x250::/ad_unit|1|photo_x::
::jseblodend_photo_x::::/jseblodend_photo_x::
::jseblod_photo_x::photo_x::/jseblod_photo_x::
::article_basic_layout|2|photo_x::Top::/article_basic_layout|2|photo_x::
::article_text|2|photo_x:: We will mainly focus on below solutions throughout the document.

(1)Analyze importance of network security and firewall in an organization
(2)Perform a comparative study for various types of firewalls operational today
(3)Improving performance of firewall
(4)Making firewall more scalable.

The document will be useful in deciding best vendor to procure firewall based on organizational requirements. It will also help network administrators to identify flaws in network security and to have its mitigation. Paper will help understand importance of network security in an organization and its compliance. Proposed design to make network more scalable will provide a base to network security researcher and encourage taking it further.

Network Firewall – Regulatory Compliance

Today, with increasing attention is paid to firewall rule-set quality due to regulations such as the ISO-27002, Sarbanes-Oxley act, CobiT framework, the Payment-Card Industry Data Security Standard (PCI DSS) and the NIST standard 800-41. All these regulations include specific sections dealing with firewall configuration, management and audit. Below are some of the criterions in Audit checklist which demands efficient firewall configuration and management.

Payment Card Industry –

ISO – 27002 Information

Control Objectives for

Data Security Standards

Security Standard

Information and related

(PCI-DSS) Requirements

Requirements

Technology (COBIT)

Requirements

1. Install and maintain a

1. Network (where business

1. Plan and Organize

firewall configuration to

partner’s and/ or third

effective, robust and

protect cardholder data

parties need access to

scalable Network Security

information system) is

policy.

2. Encrypt transmission of

segregated using perimeter

cardholder data across open,

security mechanisms such

2. Define the level of

public networks

as firewalls.

security and control that is

necessary to protect

3. Use and regularly update

2. Information security

companies' assets, through

anti-virus software or

policy should be approved

the development of an IT

programs

by the management,

governance model.

published and

4. Track and monitor all

communicated to all

3. All users and their

access to network resources

employees.

activity should be uniquely

and cardholder data

3. Should have controls

identifiable and monitored.

5. Maintain a policy that

such as firewalls, Operating

4. User access rights to

addresses information

system hardening, any

systems and data should be

security for employees and

Intrusion detection type of

in line with defined and

contractors

tools used to monitor the

documented business needs

6. Develop and maintain

system etc.

and job requirements.

4. Encryption techniques

5. Define and implement

secure systems and

applications

should be used to protect

procedures to ensure

the data.

integrity and consistency of

7. Do not use vendor-

all data stored in electronic

5. Regular assessments

form, such as databases,

supplied defaults for system

should be conducted to

data warehouses and data

passwords and other

analyze the sensitivity of

archives.

security parameters.

the data and the level of

protection needed.

::/article_text|2|photo_x::
::photo|2|photo_x::images/photos/1594/Firewall Operations and Data Flow.PNG::/photo|2|photo_x::
::photo_size|2|photo_x::Full::/photo_size|2|photo_x::
::ad_unit|2|photo_x:: ::/ad_unit|2|photo_x::
::jseblodend_photo_x::::/jseblodend_photo_x::
::jseblod_photo_x::photo_x::/jseblod_photo_x::
::article_basic_layout|3|photo_x::Left::/article_basic_layout|3|photo_x::
::article_text|3|photo_x::**KPI's of Firewalls – Comparative Study**

Firewalls fall into four broad categories: packet filters, circuit level gateways, application level gateways and stateful multilayer inspection firewalls. Commercially, there are large numbers of firewall vendors supplying different types of firewalls. Choosing the right firewall for any organization is always crucial. Listed are some of the test results performed in Test Laboratory which will provide a comparative study for various firewalls and their KPIs.

Testing setup

In order to characterize performance of firewall, below were the test environment setup used to compare performance of four most operational firewalls in market.

Cisco

Checkpoint

PF

Juniper

Platform

Cisco ASA - 5580

HP DL 380

HP DL

NS-5200

380

ASA V 8.2.2

SPLAT 2.4

Screen OS

Operating System

Checkpoint NGX

Free BSD

ASDM 6.2.5

6.1

R65 HFA 50

Multi-

Product Architecture

Multi-processor,

Multi-processor,

processor,

ASIC

Multi-core

Multi-core

Multi-

Based

core

Processing Cores

8

8

8

ASIC

Based

Gigabit Ethernet Interfaces

0

0

0

0

10 Gigabit Ethernet

4

4

4

4

Interfaces

Testing Output

Comparative analysis was mainly done considering below KPIs –

(1)Firewall Licensing – To ensure authorized use of product.
(2)Firewall Management – Ease of firewall management in distributed firewall environment.
(3)Application Intelligence – Ability of firewall to filter packets based on Application layer Intelligence.
(4)HTTP Throughput – Goal of this test is to characterize performance of system under test when deployed to protect a high performance, web based application
(5)TCP Throughput – Test included opening a TCP connection, transferring an object using HTTP and closing the TCP connection with object size 512 KB.
(6)Concurrent Connections – Number of connections handled by firewall simultaneously.
(7)UDP Throughput - Test included performance measurement of UDP throughput using 512KB domain packets.
(8)Connections per second – Number of connections handled per second.

Below are the results of the test conducted on laboratory generated traffic.

Cisco

Checkpoint

PF

Juniper

License

Proprietary

Proprietary

BSD

Proprietary

Management

Local

Centralize

Local

Local

Application Intelligence

Yes

Yes

No

Yes

HTTP Throughput (Gbps)

10.6

3.6

4.5

2.1

TCP Throughput (Gbps) (Object Size = 512

KB)

18.6

14.2

10.2

11.4

Concurrent connections

200K

250K

500K

100K

UDP Throughput (Gbps) (Object Size =

512KB)

9

4

7

2

Connections per second

182K

66K

200K

14K

Optimized Firewall Design

Based upon a recent survey of number of firewall administrators:

• Only 10% have automated techniques for analyzing errors
• 47% cited time/staffing constraints as a primary reason these issues are not addressed
• 50% feel it is likely their firewall rulebase contains undetected errors; 32% consider this a “medium” or “high” risk
::/article_text|3|photo_x::
::photo|3|photo_x::::/photo|3|photo_x::
::photo_size|3|photo_x::Full::/photo_size|3|photo_x::
::ad_unit|3|photo_x:: ::/ad_unit|3|photo_x::
::jseblodend_photo_x::::/jseblodend_photo_x::
::jseblod_photo_x::photo_x::/jseblod_photo_x::
::article_basic_layout|4|photo_x::Top::/article_basic_layout|4|photo_x::
::article_text|4|photo_x::Based on above data, we tried to optimize the firewall design considering below factors in mind –

• Design firewall rulebase such that it is consistent, correct and compact in distributed firewall environment
• To make firewall more scalable in this diverse network environment?
• Formulate analysis techniques that firewall administrators should use before and/or immediately after the deployment of a new rule to predict the likelihood that the rule will become orphaned
• Develop an auditing framework that provides an adequate degree of assurance for all phases of the firewall lifecycle

---

Optimizing Firewall Performance

Most firewalls work by inspecting packets in a sequential manner. When firewall receives a packet, it compares it against the first rule, then the second, then the third, etc.
When it finds a rule that matches, it stops checking and applies that rule. If the packet goes through each rule without finding a match, then that packet is denied. It is critical to understand that the first rule that matches is applied to the packet, not the rule that best matches. Some of the important criterions for efficient firewall rulebase design should be as follows -

1. Keep the more specific rules first, the more general rules last

2. Always use IP Address instead of name resolution of URL.

3. Protocol Session Timeout should be more aggressive and should be moderate to improve performance.

4. For larger organizations with multiple firewall administrators, following information should be put into comments whenever a rule is modified. This will help track who changed which rules, and why.
• Name of person modifying rule
• Date/time of rule change
• Reason for rule change (with task/incident number)

5. Efficiently use logging feature of firewall rule base tracking will help improving the performance.

6. After completing firewall rulebase modification, it is critical to test it. Port scan can be performed to verify correct port opening.

7. Auditing of firewall rulebase should be performed periodically. This will help removing redundant, orphaned and shadowed rules.

8. Limit the number of applications that run on the firewall in order to maximize CPU cycles and network throughput.

Increasing Scalability

Performance is not all about throughput. Scalability can also improve performance. In order to improve scalability, firewall should always be kept at corner of the network.
We can achieve higher performance using proposed design.
::/article_text|4|photo_x::
::photo|4|photo_x::images/photos/1594/Comman Error inConfigration-Firewall.PNG::/photo|4|photo_x::
::photo_size|4|photo_x::Full::/photo_size|4|photo_x::
::ad_unit|4|photo_x:: ::/ad_unit|4|photo_x::
::jseblodend_photo_x::::/jseblodend_photo_x::

::jseblod_photo_x::photo_x::/jseblod_photo_x::
::article_basic_layout|5|photo_x::Top::/article_basic_layout|5|photo_x::
::article_text|5|photo_x::Proposed is a design of a core network that interconnects the existing networks. Communication from firewall to firewall will traverse the router, greatly simplifying the design and improving scalability.
With this network design the way connectivity is achieved between the sites is irrelevant to the firewalls. All that is required of the firewalls is a dedicated interface to connect to the designed network. Scaling the network becomes a simple process of connecting new devices to the router.

Conclusion

Throughout our work, we have attempted to evaluate performance of major operational firewalls in the market today. With increasing importance of Network Security in any organization, we have summarized major regulatory compliance and need to have efficient, clean and robust firewall configuration and management. Most currently undertaken research work on firewall has been carried out theoretically and lacks practical implementation. We have attempted to compare performance of various firewalls based on practical implementation. Comparison of various firewalls will also help in selecting right vendor at time of procurement. To improve firewall performance, we have summarized key points and proposed design to increase scalability.
::/article_text|5|photo_x::
::photo|5|photo_x::images/photos/1594/Improved Firewall Scalability.PNG::/photo|5|photo_x::
::photo_size|5|photo_x::Full::/photo_size|5|photo_x::
::ad_unit|5|photo_x:: ::/ad_unit|5|photo_x::
::jseblodend_photo_x::::/jseblodend_photo_x::

::moderation_status::0::/moderation_status::
::isratingchanged::0::/isratingchanged::
::old_rating::0::/old_rating::
::mod_comment:: ::/mod_comment::
::attachment::::/attachment::
::attachment_x::
::/attachment_x::
::jseblodend::::/jseblodend::