



# MASTER THESIS



# Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

Master Thesis in Computer Network Engineering

May 2013

Author: Su Wenhui & Xu Junjie

Supervisor: Olga Torstensson

Examiner: Tony Larsson

---

School of Information Science, Computer and Electrical Engineering  
Halmstad University  
PO Box 823, SE-301 18 HALMSTAD, Sweden

© Copyright Wenhui Su & Junjie Xu(author), 2013(year). All rights reserved  
Master Thesis  
Report, IDE1302  
School of Information Science, Computer and Electrical Engineering  
Halmstad University

## Preface

This thesis work is a practical guide which demonstrates what the firewall performance evaluation is and how various parameters are collected and examined. Comparisons of two mainstream firewall solutions, hardware-based and software-based, are presented. It is also a good study material for the firewall beginners or firewall potential customers who learn some basic concepts of firewalls and their management tools. Overall, the ideas in this thesis contribute to them how to choose a right firewall product.

We sincerely express our gratitude to our supervisor Olga Torstensson and professor Tony Larsson for their supervision and assistance during our thesis writing. We also thank IDE department, Halmstad University for providing equipment and such opportunity to complete this thesis.



## Abstract

A firewall is an essential component to provide network security and traffic control. It is widely used to prevent illegal accesses to private or corporate networks from external unsafe source like Internet. Firewalls are basically classified into two types, hardware firewalls and software firewalls. Hardware-based is a single external hardware to a system, but software-based is installed on a computer inside a system. Two such firewalls, Cisco ASA 5505 and Linux iptables are implemented and practical evaluated their performance. The performance test in this paper work primarily focuses on Network layer, and the main parameters include Throughput, Latency, and Concurrent Sessions. Different performance monitoring tools are also introduced in this paper.

As a network layer firewall, the most impressive feature is through inspecting the packets to manage the traffic from the higher Layer 4-7 of OSI (Open Systems Interconnection) model, which inevitably has a certain impact on the performance. The bottleneck of the whole network is determined by what extent the impact is. The primary objective of this thesis is through analyzing the test reports to evaluate the two type firewalls' performance. Thus the results reported in this paper gives some ideas to new firewall customers about what aspects should be considered before selecting a suitable firewall product.



## Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Motivation.....	2
1.2	Goal .....	3
1.3	Limitation .....	3
1.4	Methodology .....	4
1.5	Required Resources .....	4
1.6	Structure of Thesis.....	5
<b>2</b>	<b>Background .....</b>	<b>7</b>
2.1	Firewalls.....	7
2.1.1	Cisco ASA 5505 .....	8
2.1.2	Linux iptables .....	9
2.2	Tools.....	10
2.2.1	ntop.....	10
2.2.2	Cisco ASDM.....	13
2.2.3	Cisco Pagent router .....	15
2.2.4	Nginx .....	16
2.2.5	Webbench.....	18
2.3	Network layer performance test.....	19
2.3.1	Throughput.....	20
2.3.2	Latency .....	20
2.3.3	Concurrent Sessions .....	21
<b>3</b>	<b>Implementation .....</b>	<b>23</b>
3.1	The implementation of the throughput test.....	23
3.1.1	Topology of throughput test.....	24
3.1.2	The test condition and items in throughput test.....	24
3.1.3	The limitation in throughput test.....	27
3.2	The implementation of the latency test .....	27
3.2.1	Topology of latency test.....	28
3.2.2	The test condition and items in latency test .....	28
3.2.3	The limitation in latency test .....	29
3.3	The implementation of the concurrent sessions test.....	30
3.3.1	Topology of concurrent sessions test .....	30
3.3.2	The test condition and items in concurrent sessions test.....	30
3.3.3	The limitation in concurrent sessions test .....	31
<b>4</b>	<b>Results.....</b>	<b>33</b>
4.1	Comparison of throughput results.....	33
4.1.1	Fixed packet length under the highest sending rate and burst off setting .....	33
4.1.2	Random packet length under the different sending rate without burst.....	35
4.1.3	Random packet length under the different sending rate with burst .....	37
4.2	Comparison of latency results .....	39
4.3	Comparison of concurrent sessions results .....	40
<b>5</b>	<b>Conclusion.....</b>	<b>45</b>



<b>Reference .....</b>	<b>48</b>
<b>Appendix.....</b>	<b>51</b>

## Figures

Figure 1. Diagram for performance testing.....	4
Figure 2. Cisco ASA 5505 flash files status .....	14
Figure 3. Concurrent session test website.....	18
Figure 4. Two kinds of firewall throughput test topology.....	24
Figure 5. Two kinds of firewall latency test topology .....	28
Figure 6. Two kinds of firewall concurrent sessions test topology .....	30
Figure 7. The maximum throughput of Cisco ASA 5505 with different fixed packet length...	34
Figure 8. The maximum throughput of Linux iptables with different fixed packet length .....	35
Figure 9. The sending rate versus Packet length .....	35
Figure 10. Cisco ASA 5505 throughput with random packet length and different fixed sending rate without burst .....	36
Figure 11. Linux iptables throughput with random packet length and different fixed sending rate without burst.....	36
Figure 12. Cisco ASA5505 firewall in burst on state in throughput test .....	38
Figure 13. Linux iptables firewall in burst on state in throughput test.....	38
Figure 14. Average delay in latency test.....	40
Figure 15. The number of average failures in two firewalls with different clients request ....	42
Figure 16. Cisco ASA 5505 system resources status .....	42
Figure 17. Linux iptables server resources status.....	43

## Tables

Table 1. Required resources in testing.....	5
Table 2. IP address table for throughput test .....	25
Table 3. Pagent TGN destination MAC address.....	25
Table 4. Rules in the firewall for testing.....	26
Table 5. IP address table for latency test.....	29
Table 6. IP address table for concurrent sessions test .....	31
Table 7. The max Throughput with the fixed packet length.....	34
Table 8. The average delay in two kinds firewall with different data-length.....	39
Table 9. The test result in two firewall platform with different clients request .....	41



# **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

## **1 Introduction**

With the rapid development of computer technology and communication technology, the network is gradually changing the way of people's work and life. Network openness, connectivity and expansion of sharing, especially the emergence of the Internet impact a lot on the society and the importance of networking are also growing. With the rise of network e-commerce, e-payment, and other new network business, network security issues become increasingly important. In addition, with the continuous expansion of network scale and increasing complexity, the users' requirement on the network performance is growing. Therefore, network management has gradually become a critical task in the development of network technology.

Since people invented the Internet, resource sharing and information security has contradictorily existed with each other. The more people use network resource sharing, the more critical it becomes to further strengthen the information security. The enterprises start to encounter a variety of computer viruses and hackers attack. Numerous examples show that many websites have been damaged. With the wide application of computer systems, more and more people are using the system, however, education and training is often not keep up with the needs to update people's knowledge; operators, programmers and administrators' mistakes or lack of experience will cause the security bugs of the system. The emergence of the firewall makes the network security control becomes possible. The firewall is a security barrier between the protected network and an untrusted network, used to protect the internal network and resources. It establishes a security control point between the internal and external networks, to control and audit services and access into and out of the internal network.

The applications of diverse firewall products are becoming popular to improve the network security and the traffic management. To meet their special requirements,

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

customers always refer some evaluations or comparisons results before choosing a right firewall product. The progress of evaluation includes many aspects according to different needs. In general four factors are considered during the evaluation: security, network performance, network functionality and management. The Network performance is the basis to ensure the end user's bandwidth and many network applications can be achieved. Along with the rapid development of the computer network, the network performance is becoming more and more important for both the customers and vendors.

On market there are many types of firewall products classified by their software structures or different usages in a network. The most common one is Network layer firewall also known as packet filters firewall. Such kind of firewall works at a relatively low level of the TCP/IP protocol stack; it deny packets to pass through the firewall unless they match the committed rules and policies. The rules and policies may be committed by firewall administrator or with default setting. [1] Two sets of such firewall platform were tested, one is single hardware based firewall Cisco ASA 5505 and another is software based firewall Linux iptables installed on a server.

### **1.1 Motivation**

The firewall products are diversified according to different types of traffic and required functions. The two popular firewall solutions existing on the market are single hardware-based and software installed on a server. No matter which types of the firewalls are, usually they are placed on the edge of the core or enterprise network. Obviously, the performance of the firewall has a decisive impact on normal applications of network and the actual bandwidth that end users should achieved. Meanwhile there is no standard method of performance measurement. Even to test the same parameters, different manufacturers also have their own implementations and methods.

# **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

Considering various firewall brands, solutions and performance measurement methods, how to choose a right firewall product to meet some special requirements is always a practical problem in front of a customer. Firewall performance evaluation becomes important for customers purchasing firewall product or vendor producing.

## **1.2 Goal**

The primary objective is through comparing the performances of two different firewalls in order to investigate the advantages and disadvantages of each type. The task includes implementations of two firewall platforms: Cisco ASA 5505 which belongs to the pure hardware-based and software-based firewall product Linux iptables. The second is to study different firewall performance monitoring tools. Finally, for the potential firewall customers or the firewall beginners, the testing results and the conclusions of this thesis contribute to their decisions making before deploying a proper firewall product in their own networks.

## **1.3 Limitation**

Both firewall products used for this evaluation belong to the SME (Small and Medium Enterprises) class providing the highest 100Mbps Fast Ethernet ports. According to the hardware resource and deadline, the implementations in this thesis are focusing on the three performance parameters: throughput, latency and concurrent sessions. The equipment used for testing firewall performance are not professional instruments but the limited devices in our laboratory, for example the traffic generator, simulating real data stream from an unsecured source, is not able to create all the needed traffic. In addition, the memory size and the processing power of the computers are a little bit low. The testing results maybe have slight deviation comparing with product manual due to the differences of applied testing rules and traffic types.

# Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

## 1.4 Methodology

First, according to the existing conditions of the laboratory and the firewall performance evaluation recommendations from IETF (The Internet Engineering Task Force) RFC 1242/2544 to determine the test parameters.[2][3] Throughput, latency and concurrent sessions, three network layer performance parameters are selected as the main objects to study in this thesis. Second, two different implementations are taken to test the two firewall system individually shown as Figure 1.[4] The lower part with traffic generator is used for the throughput and latency test, and the upper is measuring the numbers of concurrent sessions through a client generating requests of session to a corresponding server.

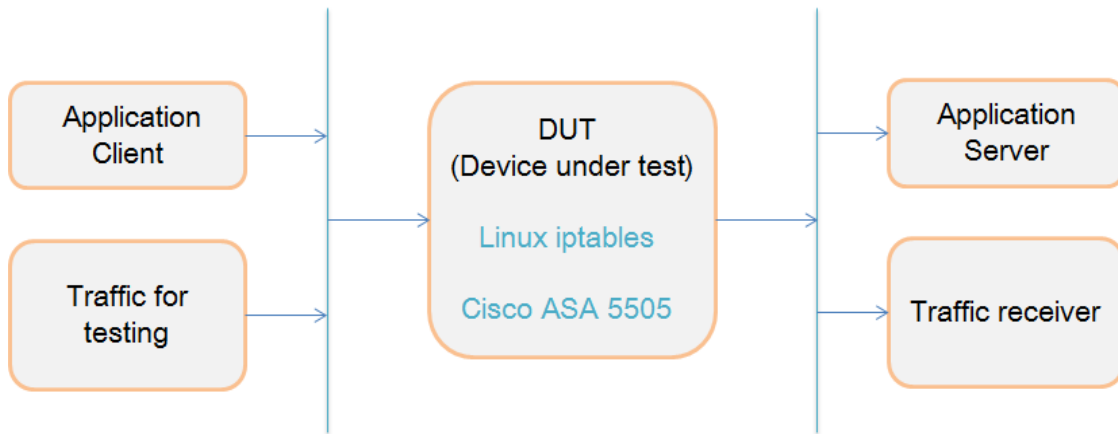


Figure 1. Diagram for performance testing

The last, considering the consistency of the testing, both monitoring systems are the same and independent from the firewall platforms to avoid taking up the processing and memory resources of the firewalls.

## 1.5 Required Resources

To set up the testing environment, two firewall platforms, one traffic generator and four PCs are needed. Detailed information is listed below (Table 1):



## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

Name	Device	Function	Model	CPU	Memory	Storage	OS
PC1	Linux iptables	Software based firewall	Dell Desktop OPTIPLEX 740	AMD Athlon(tm) 64 X2 Dual Core Processor 4600+ (2.4Ghz)	2GB	Hard disk 160GB	CentOS 6.3
PC2	ntop server	Network traffic monitor & http server	Dell Desktop OPTIPLEX 740	AMD Athlon(tm) 64 X2 Dual Core Processor 4600+ (2.4Ghz)	2GB	Hard disk 160GB	CentOS 6.3
PC3	Webbench server	Concurrent session generator	Dell Laptop LATITUDE D630	Intel(R) Core(TM)2 Duo T7300 @2.0Ghz 2.0Ghz	2GB	Hard disk 120GB	ubuntu 12.04 LTS
Firewall	Cisco ASA 5500 Series	Hardware based firewall	ASA5505	Geode 500 MHz	512MB	Flash 128MB	Cisco IOS ASA 8.2(5)
Router	Cisco Pagent Router	Traffic generator (TGN&NQR)	Cisco 2811 router	FCZ102470GH	512MB	ATA CompactFlash 64MB	Cisco IOS 2800 12.4
PC4	PC	ASDM monitor 6.4(5)	Dell Desktop OPTIPLEX 790	Intel(R) Core(TM) i5-2400 CPU @3.1Ghz 3.1Ghz	8GB	250GB	Windows 7 Enterprise

Table 1. Required resources in testing

### 1.6 Structure of Thesis

The content in our thesis is categorized as follows: chapter 2 introduces the background work including the basic concepts of different types of firewall solutions and the definitions of different performance parameters. The detailed descriptions about different kind of tools are also presented. Chapter 3 deals with the implementation work, which consists of different traffic generators, http server, monitoring tools and the configurations of two firewall systems. Chapter 4 presents the evaluation results of the two firewall platforms. Finally, this report ends with the conclusion and what the problems should be considered before deploying a firewall product for potential users.

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

# Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

## 2 Background

The general developing tendency of the Internet bandwidth is increasing quickly with a certain speed. The upgrade of the network structure is also very frequent, but network security is a constant factor along with these changes. Firewall products are always put on the edge of a network as gateway providing security, its performance determines the bandwidth efficiency and the cost of a network. However, there is no standard method to perform firewall evaluation. A well-known and recommended test method is RFC 2647 Benchmarking Terminology for Firewall Performance. [5]

### 2.1 Firewalls

A firewall is a device widely used to provide network security by rejecting unauthorized traffic from an untrusted source such as Internet; meanwhile authorized traffic is verified to pass through according to different types of rules and policies. Normally firewalls exist in the form of a single hardware device or a software entity. Although there are many Firewall technologies, but in general they can be divided into two categories, packet filtering and application-proxy. [6]

The Packet filtering firewalls work at the network layer and the transport layer of the OSI network reference model, which is according to analyzing the information in the packets header such as the Source IP address, Destination IP address, Source and Destination port number, transport protocol (TCP, UDP, ICMP, etc.), ICMP message, etc. to determine whether the packets are allowed to pass through or not. Only packets that meet the filter rules are forwarded to the appropriate destination, the rest of the packets were discarded from the data stream. [7] Although Packet filtering is a general-purpose, low-cost and effective means of security, its weakness is obvious. Because the filtering rules are based only on the network layer and the transport layer with the limited information, therefore it is impossible to fully meet various security requirements. [8] Furthermore the number of filtering rules is also limited; the performance greatly influenced as the number of rules increasing.

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

Packet filtering firewalls lack of audit and alarm mechanisms to verify the user's identity, thus they are susceptible to spoofing attacks. [9]

Application-Proxy Firewalls are working on the highest layer of the OSI reference model, application layer. The network traffic flow is completely obstructed by a special agent of each application service which monitors and controls the traffic of application layer. All the packets that need to pass through this type of firewall are checked and compared to the rules configured in the firewall. If the packet is qualified then it is recreated and sent out. Because each packet is renewed, it is potential that an application-proxy firewall can prevent unknown attacks based upon weaknesses in the TCP/IP protocol suite that a packet filtering firewall would not prevent. The drawback is that a separate application-proxy must be written for each type of application being proxy examined. An HTTP proxy for web traffic, an FTP proxy for file transfers, a Gopher proxy for Gopher traffic, and so on are needed. [10]

### **2.1.1 Cisco ASA 5505**

The Cisco ASA (Adaptive Security Appliance) 5500 Series give the solutions that specifically designed to the highest safety and excellent VPN services. With innovative scalable service architecture, it is the core component of the Cisco Self-Defending Network. The Cisco ASA 5500 Series can provide proactive threat defense, network activity control and application traffic control. It also delivers flexible VPN connection. The lower models are not only for protection of the home office or branch office but also can protect the small and medium-sized enterprises. The higher models can protect the large enterprise networks and give them depth security protection. [11] It can reduce the overall deployment costs and operating complexity.

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

Cisco ASA 5505 Adaptive Security Appliance is a next-generation, full-featured security equipment. It is suitable for small businesses, branch offices and medium-sized enterprise. It provides IPSec, SSL VPN and rich networking services. [6] Using the integrated Web-based Cisco Adaptive Security Device Manager, it can quickly deploy and easily managed. Cisco ASA5505 is equipped with 8 10/100Mbps Fast Ethernet ports. It provides two PoE (Power over Ethernet) ports, which suitable for PoE devices such as IP phones or cameras. It is similar to the other Cisco ASA 5500 Series devices which have modular design. It has an external expansion slot and multiple USB ports that can be added more services in the future.

### **2.1.2 Linux iptables**

Netfilter/iptables (referred as iptables) is a packet filtering firewall in Linux platform. It is free which the same as other majority of Linux software. It can perfectly replace the expensive commercial firewall solutions. Linux iptables support packet filtering, packet redirection and NAT (Network Address Translation) etc. [12]

The iptables packet filtering system is a powerful tool that can be used to add, edit and remove the rules which are the conditions predefined by network administrator. The packet filtering system makes the decision followed by the rules composition. These rules which specify the source address, destination address, transport protocol (TCP, UDP, ICMP) and the type of service (such as HTTP, FTP and SMTP, etc.) are stored in the kernel space packet filtering table which are integrated in the Linux kernel.

Netfilter/iptables is referred as a single entity, but it is actually made up by two components: netfilter and iptables. The relationship between them is very easy to confuse. In fact, iptables is only the Linux firewall management tool located in /sbin

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

/iptables. The one who realize the firewall features is netfilter. It is the internal structure which achieves the packet filtering in the Linux kernel. [12]

CentOS (Community ENTERprise Operating System) is one of the Linux distributions. It has already built the iptables in it. The iptables requires elevated privilege to operate and must be executed by root user.

### **2.2 Tools**

According to the functionality of these tools, they can be classified into two categories, one is for monitoring the network traffic or log reports; another is used for generating test traffic. The test traffic is manually configured with special overhead bytes or compositions. The ntop is developed on Linux operation system for network traffic monitoring. ASDM (Adaptive Security Device Manager) is a Cisco's property used for management of Cisco ASA series firewall products. Cisco Pagent router is a traffic generator for testing purpose. TGN (Traffic GeNerator) and NQR (Network Quality Reporter) are the main applications of Pagent router, which play an important role to test the throughput and latency. The Webbench and Nginx are used to set up the http client and server respectively for the concurrent sessions test.

#### **2.2.1 ntop**

ntop is an open source monitoring tool for network traffic. It is easy to use and suitable for monitoring various kinds of networks. It is a flexible and full-feature tool used to monitor and resolve LAN problems. The ntop even can list the utilization of each node network bandwidth. It provides a command-line input and the web interface; it also can be applied to the embedded web services. [13]

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

ntop works like a network sniffer. It has an irreplaceable role to assist in the monitoring of network data transmission and network troubleshooting. By analyzing the network traffic bottleneck effect or performance degradation, it can find the problems which exist in the network. It can also be used to determine whether the hackers are attacking the network system. If you suspect that the network is being attacked, the ntop can determine what type of the packet and the source of the packet. Then it can let the network administrator take the action or make the appropriate adjustments to the network to ensure the safety and efficiency.

ntop is more intuitive than some other network monitoring software. It shows detailed information about network traffic. The network administrator can easily determine which traffic belongs to a particular network protocol, the major traffic belongs to which host, the packet transmission time between source and destination. This valuable information gives an overview of network to the administrator who can determine the network problems and optimize network performance immediately.

Now the ntop can run in Linux platform and Windows platform. The ntop 5.0.1 for Linux is installed in our lab.

The installation steps are as follows:

1. Before starting the ntop installation, these associated packages should be installed at first as below.

```
yum install libpcap
yum install libpcap-devel
yum install libxml2
yum install libxml2-devel
yum install libpng
yum install libpng-devel
yum install pango
yum install pango-devel
yum install gdbm-devel
yum install rrdtool
yum install rrdtool-devel
```

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

```
yum install libtool
yum install gcc gcc-c++
yum install gdbm gdbm-devel
yum install zlib zlib-devel
yum install GeoIP GeoIP-devel
yum install subversion
yum install python
```

2. Download the ntop software from [www.ntop.org](http://www.ntop.org) .The version is top-5.0.1.tar.gz for Linux.

3. Upload the file to the directory: /var/www and compile it.

```
tar zxvf ntop-5.0.1.tar.gz
cd ntop-5.0.1
ls
./autogen.sh
make
make install
```

4. Create the ntop user and group.

```
groupadd ntop
useradd ntop -g ntop
```

5. Create the ntop rrd directory which for ntop use.

```
mkdir /usr/local/var/ntop/rrd
chown -R ntop:ntop /usr/local/var/ntop/rrd
```

6. Change the owner and group of these two directories to ntop.

```
chown -R ntop.ntop /var/www/ntop/share/ntop
chown -R ntop.ntop /var/www/ntop/var/ntop
```

7. Start the ntop service

```
ntop -u ntop -d
```

8. Setup the auto-start for Linux start



## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

```
vim /etc/rc.local
```

Add:

```
/usr/local/bin/ntop -u ntop -d
```

9. Now open the browser and type "localhost:3000". There is the ntop web management interface. The default username and password are admin.

### 2.2.2 Cisco ASDM

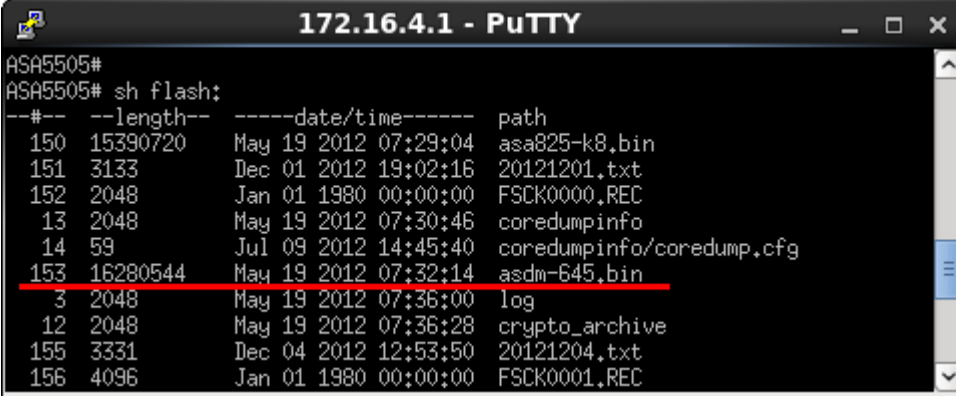
Cisco's ASDM (Adaptive Security Device Manager) is the graphic tool which used to manage the Cisco ASA Adaptive Security Appliances and Cisco PIX appliances, providing security management and monitoring services. Cisco ASDM provides intelligent wizard and friendly user interface. It has web-based security design and enables user access Cisco ASA firewall in anytime and anyplace.

Its setup wizards can help you configure and manage Cisco firewall devices without cumbersome command-line scripts. "It has powerful real-time log viewer and monitoring dashboards that provide an at-a-glance view of firewall appliance status and health status." [14]

The installation steps are as follows:

1. First, the flash on the firewall (Cisco ASA 5505) must be checked using command "show flash" in the Privileged EXEC mode (Figure 2) to make sure it has the ASDM image. If there is no file called asdm-xxx.bin, it means to be downloaded from Cisco website and save it on the flash. The ASDM version is 6.4 in the thesis (5).

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions



--#--	--length--	-----date/time-----	path
150	15390720	May 19 2012 07:29:04	asa825-k8.bin
151	3133	Dec 01 2012 19:02:16	20121201.txt
152	2048	Jan 01 1980 00:00:00	FSC0000.REC
13	2048	May 19 2012 07:30:46	coredumpinfo
14	59	Jul 09 2012 14:45:40	coredumpinfo/coredump.cfg
153	16280544	May 19 2012 07:32:14	asdm-645.bin
3	2048	May 19 2012 07:36:00	log
12	2048	May 19 2012 07:36:28	crypto_archive
155	3331	Dec 04 2012 12:53:50	20121204.txt
156	4096	Jan 01 1980 00:00:00	FSC0001.REC

Figure 2. Cisco ASA 5505 flash files status

2. Setup the management vlan and apply it to the corresponding Ethernet interface on the firewall.

```
interface Vlan99
nameif management
security-level 0
ip address 192.168.1.1 255.255.255.0
```

```
interface Ethernet0/7
switchport access vlan 99
no shutdown
```

3. Create the management user and password.

```
username cisco password cisco
```

4. Open http service and configure the permission network.

```
http server enable
http 192.168.1.0 255.255.255.0 management
```

5. Connect the monitor PC to the management Ethernet port and set the PC's IP address 192.168.1.3/24.

6. Open a browser and type "<https://192.168.1.1/>" then the Cisco ASDM option interface appears, selecting "Run ASDM" with the username and the password *cisco*.

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

### **2.2.3 Cisco Pagent router**

Cisco Pagent router is a Cisco router installed with the Cisco Pagent IOS image which contains both Advanced IP and IP Base Services. The IP traffic generation tools generates realistic traffic and bottlenecks in order to test QoS features such as IP Classification, IP Marking, and Queuing, etc. The Pagent image can be used to send or receive traffic and to analyze the bandwidth used by network interface. Cisco Pagent IOS was developed within Cisco primarily and was only intended for Cisco internal users. The versions 2621 and 2801 of Patent router have been permitted to use in CCNP Academies with special permission from Cisco's Pagent group. In this thesis work, two main function tools, TGN and NQR, are utilized to generate certain amount of traffic with required protocols. [15]

#### **TGN (Traffic GeNerator)**

Traffic GeNerator is a Pagent IOS image based test tool, which defines and sends packets on any combination of supported interfaces from a router. TGN has predefined templates for specific packet types. [16] In this thesis TGN is used to generate huge amount of traffic with different configurations to test the network throughput parameter.

#### **NQR (Network Quality Reporter)**

"NQR is an IOS-based program in the Pagent test tool set. It is a simple tool that measures end-to-end network delay, jitter, packet drop, and out-of-sequence packets. Packets are sent from an NQR router into a network, which is configured to route the packets back into one of the interfaces of the NQR router. NQR processes the returned packets and calculates the necessary statistics. [17]" The special packets

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

which contain functional overhead bytes have been predefined. Timestamp is one type of these functional bytes, which can be added into NQR packet. After sending the packet, it records the capture time of the packets thus necessary network delay is calculated. The firewall latency test is the main application of NQR in this thesis.

### **2.2.4 Nginx**

Nginx (pronounced "engine X") is a lightweight HTTP server software which written by Russians. It is a high-performance HTTP and reverse proxy server. It is also an IMAP/POP3/SMTP proxy server. [18] Nginx is famous for its stability, rich library of modules, flexible configuration and low consumption of system resources. It is licensed under a BSD-like license and it can run on Unix, Linux and Microsoft Windows.

It has many superior features. As a Web server which compare to Apache, Nginx using fewer resources to support more concurrent connections, reflecting the higher efficiency which especially welcomed by web host provider. It can support up to 50,000 concurrent connections response. [19]

The installation and configuration of Nginx are relatively easy. It supports 7\*24 hours of uninterrupted operation even running several months without restart. It also supports in service upgrading.

The installation steps are as follows:

1. Download the rpm package for CentOS 6.3 which from nginx website.  
(<http://nginx.org/en/download.html>)

```
wget http://nginx.org/packages/centos/6/noarch/RPMS/nginx-release-centos-6-0.el6ngx.noarch.rpm
```

2. Install this rpm package and ignore the warning.

```
rpm -ivh nginx-release-centos-6-0.el6ngx.noarch.rpm
```

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

3. Install the nginx and enter “y” for all the requests. After the installation is finished, it prompts "Complete!" for the successful installation.

```
yum install nginx
```

4. Start the nginx service

```
/usr/local/nginx/sbin/nginx
```

Open a browser and enter “<http://127.0.0.1>”, if the words “Welcome to nginx!” appears, it means the service is successfully started with the default homepage.

5. Using command “whereis nginx” to check the directory of nginx.

```
[Admin@224-49 Desktop]$ whereis nginx  
nginx: /usr/sbin/nginx /etc/nginx /usr/share/nginx
```

The homepage is in the /usr/share/nginx/html directory. For the purpose of testing the concurrent session, a new homepage is created to replace the original index.html file from that directory.

6. Reload the page and check the result. If the nginx server works well, the page shows correctly as Figure 3.

# Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

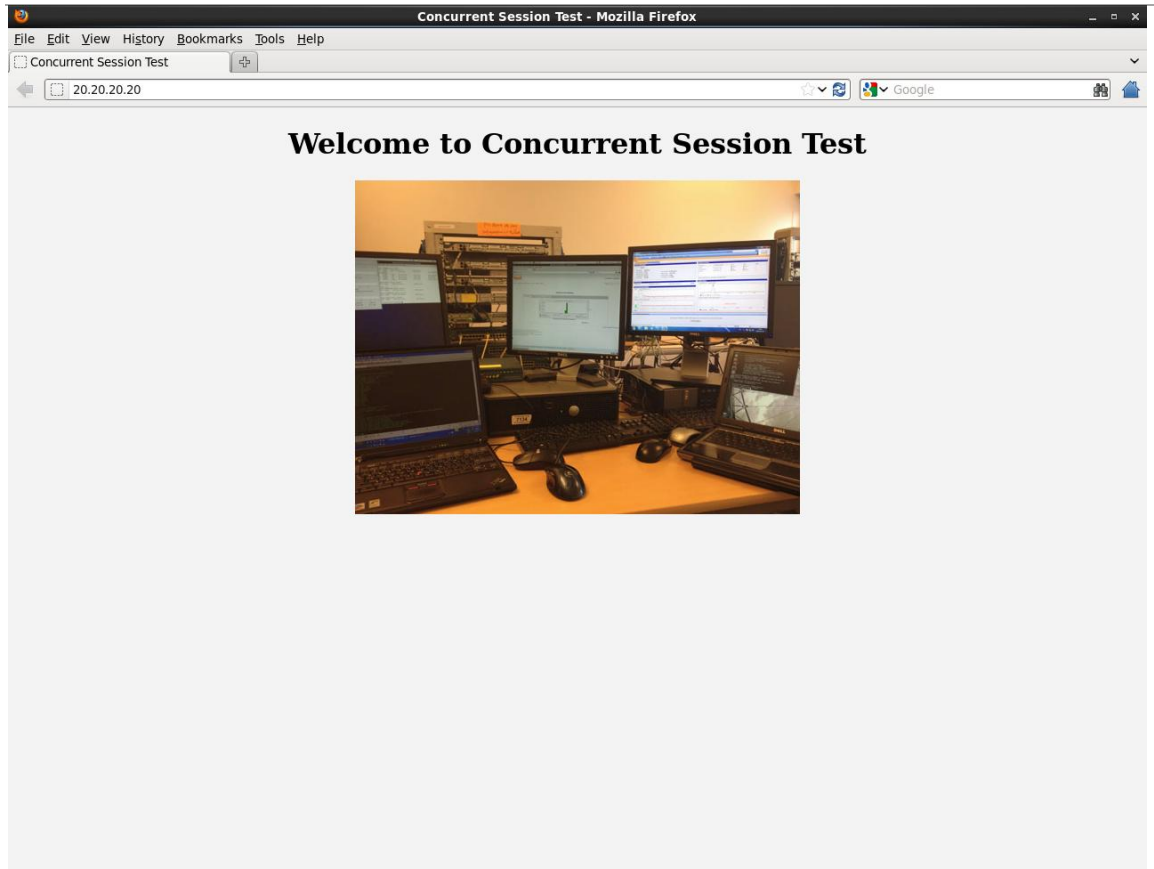


Figure 3. Concurrent session test website

## 2.2.5 Webbench

Webbench is a well-known website pressure testing tool, which is developed by Lionbridge. Webbench can be used testing the performance of the different services on the same hardware or testing the same service on the different hardware. It can show two parameters in a standard test, the number of requests per second and the amount of data per second. [20]

Webbench not only has the ability of testing the static pages, but also has the ability of testing dynamic pages (ASP, PHP, JAVA, and CGI). It also supports to test the performance of SSL security website whether static or dynamic, such as e-commerce websites.

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

Webbench can simulate up to 30,000 concurrent connections to test the loading capacity of the website.

The installation steps are as follows:

1. Download the Webbench tar file and compile it

```
wget http://home.tiscali.cz/~cz210552/distfiles/webbench-1.5.tar.gz
tar zxvf webbench-1.5.tar.gz
cd webbench-1.5
make && make install
```

2. Check whether it works.

```
webbench -c 500 -t 30 http://20.20.20.20/
```

Parameter Description:

-c represents the number of concurrent

-t represents the time (seconds)

3. When the terminal displays the results as below, it means the Webbench is working well and ready for the tests.

Webbench – Simple Web Benchmark 1.5

Copyright (c) Radim Kolar 1997-2004, GPL Open Source Software.

Benchmarking: GET http://20.20.20.20/

500 clients, running 30 sec.

Speed=3230 pages/min, 11614212 bytes/sec.

Requests: 1615 succeed, 0 failed.

### **2.3 Network layer performance test**

The network layer performance test refers to the performance test of a firewall forwarding the data packet. The RFC 1242/2544 is the primary reference standard in this test which is including throughput, latency, packet loss rate, and back-to-back buffer as the basic four aspects. Considering the limitation of the testing devices, three parameters are selected from IETF recommendation: Throughput, Latency and Concurrent sessions. These indicators actually focus on the performance

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

comparison between different network devices under the same testing conditions, rather than the actual throughput. [2][3]

### **2.3.1 Throughput**

The data stream of the network is composed of numerous frames. The firewall consumes resources to process each frame. The throughput refers to the maximum rate that the firewall can receive and forward without any frame loss. The IETF RFC 1242 gives the standard definition of throughput: "The maximum rate at which none of the offered frames are dropped by the device." Clearly the throughput is the maximum data frame forwarding rate without any packet loss. The size of the throughput is mainly determined by the Ethernet cards and the efficiency of the programmed algorithm within the firewall. An un-optimized algorithm requires the firewall system with a large number of operations so that traffic is greatly reduced. [2]

### **2.3.2 Latency**

Different types of network applications are very complex; many of them are very sensitive to latency (such as audio, video, etc.). Adding the firewall into the network inevitably increases the transmission delay, so a firewall with the low latency is a must.

The two firewall products belong to store-and-forward devices which must receive a complete packet before they start forwarding so its delay depends on the packet size. The bigger packet size, the larger delay; vice versa. IETF RFC 1242 3.8 gives the definition of Latency and the calculation methodology. For the devices using store-and-forward method according to the calculation of delay defined as LIFO (last in, first out) which is to measure the time interval between the last byte of the input



## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

data frame comes into the input port and the first byte of the data frame comes out of the output port. [2]

### **2.3.3 Concurrent Sessions**

The number of concurrent connections is an important aspect to evaluate the performance of the firewall. The number of concurrent connections defined in IETF RFC 2647 refers to the maximum number of connections established between the hosts through the firewall or between the host and the firewall at the same time. It indicates the access control capability to connect to multiple connections and the state tracking capability of the firewall. [5]

The number of this parameter directly links to the maximum information size that the firewall can support. Like the routing table which stores routing information from the router, the concurrent connection table stores the concurrent connection information from the firewall. It can dynamically allocate the memory space of the process after the firewall system is enabled. A larger concurrent connection table can increase the maximum number of concurrent connections of the firewall, and allows the firewall supporting more client terminals. Although it seems that the bigger the number of concurrent connections firewall the better, meanwhile, too large concurrent connections table bring negative effects: the consumption of system memory and processing resources are more.

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

# Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

## 3 Implementation

In this part, we introduce the implementation details about the firewall performance test of throughput, latency and concurrent sessions separately. It contains the test topologies, the physical connections and the configurations of these devices which used during the test process.

As mentioned in the methodology part before, the two kinds of firewall should be test individually. To be fair, they use the same topology and the same scenario for the same parameter test. The only difference is firewall platform. The purpose is that to make a simple topology to minimize the interference of external causes as much as possible in order to approach the actual performance of the firewall.

### 3.1 The implementation of the throughput test

The implementation of this parameter testing is according to IETF RFC 2544. For a firewall device, the throughput is mainly impacted by two factors, the programmed algorithm and the hardware performance such the speed of Ethernet card, etc. Considering these aspects, the configuration of test traffic is divided into three cases which are deployed on the same number of rules:

- Fixed packet length under the highest sending rate and burst off setting
- Random packet length under the different sending rate without burst
- Random packet length under the different sending rate with burst

One of the functionality of Cisco Packet generator, TGN works as the generator creating the above traffics. Finally, through analyzing the composition and the amount of output traffic, the performance of throughput and the behaviors of each firewall products are uncovered.

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

### 3.1.1 Topology of throughput test

According to the lab condition, the Cisco Pagent router's TGN (Traffic GeNerator) program is used to generate the huge traffic. Then the traffic goes through the firewall reaching to the ntop server which measures how much traffic received.

The *inside* network is defined as the traffic sending from Pagent Fa0/0 port arrives at the port e0/0 on the firewall ASA 5505 or eth0 on Linux iptables. And then the packets go through the firewall coming out of e0/2 on ASA 5505 or eth1 on Linux iptables. The ntop server analyzes the arriving traffic in order to provide the statistics of the traffic information.

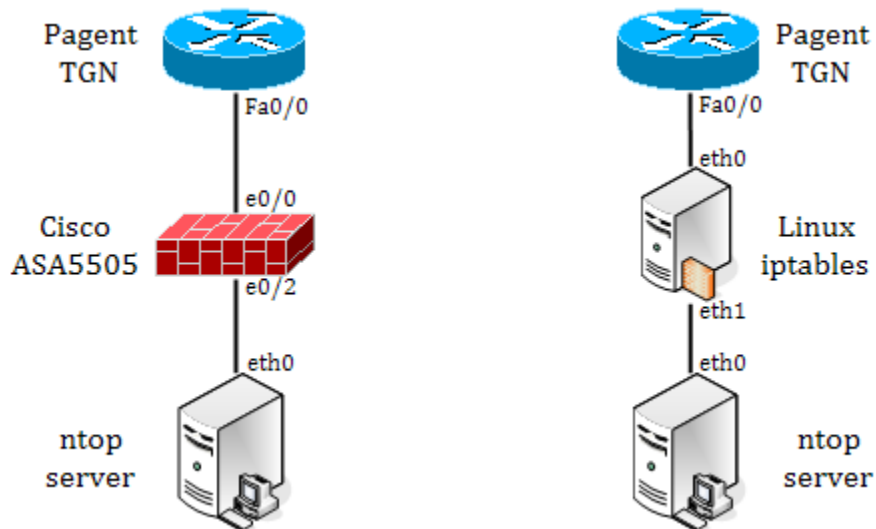


Figure 4. Two kinds of firewall throughput test topology

### 3.1.2 The test condition and items in throughput test

The IP addresses are configured in accordance with the Table 2. The 10.10.10.0/24 is used as inside network and the 20.20.20.0/24 is used as outside network. After setting up the Linux platform, the IP addresses are activated by using the command “service network restart”.

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

Device	Port	IP address	Subnet mask
Cisco Pagnet TGN	Fa0/0	10.10.10.10	255.255.255.0
Cisco ASA 5505	e0/0 (inside)	10.10.10.1	255.255.255.0
Cisco ASA 5505	e0/2 (outside)	20.20.20.1	255.255.255.0
Linux iptables	eth0 (inside)	10.10.10.1	255.255.255.0
Linux iptables	eth1 (outside)	20.20.20.1	255.255.255.0
ntop server	eth0	20.20.20.20	255.255.255.0

Table 2. IP address table for throughput test

The right MAC addresses should be set in the TGN configuration. For example, in Figure 4 Cisco ASA 5505 test part, the TGN destination MAC address should be the port of e0/0(Table 3): l2-dest a44c.11db.48c7

Device	Port	MAC address
Cisco ASA 5505	e0/0	a44c.11db.48c7
Linux iptables	eth0	0018.8b83.3d3d

Table 3. Pagnet TGN destination MAC address

The basic configuration of Cisco Pagnet TGN for three cases of throughput test is:

```
fastethernet0/0
add tcp
l2-dest 0018.8b83.3d3d
l3-src 10.10.10.10
l3-dest 20.20.20.20
l4-dest 23
add fastethernet0/0 1
l4-dest 80
data ascii 0 GET /index.html HTTP/1.1[27]
```

Under the first case, fixed packet length under the highest sending rate and burst off, the additional settings is:

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

rate 4294967295 (the maximum of rate which the TGN can generate)  
length 64, 128, 256, 512, 1518

In random packet length (the packet length ranges from 16 bytes to 1500 bytes) under the different given rate without burst and with burst cases, the additional setting is:

rate 1000, 10000, 100000, 1000000, 10000000, 100000000, 1000000000, 4294967295  
(the maximum of rate which the TGN can generate)  
length random 16 to 1500  
burst off or on  
burst duration on 1000 to 10000  
burst duration off 5000 to 10000[11]

To ensure the fair test, the same rules in Table 4 are applied to the different firewall platforms. It only allows the host 10.10.10.10 to visit the outside server 20.20.20.20 with the ping, telnet and http service.

Device	Rules in the firewall for testing
Cisco ASA 5505	access-list 111 extended permit tcp host 10.10.10.10 host 20.20.20.20 eq www access-list 111 extended permit tcp host 10.10.10.10 host 20.20.20.20 eq telnet access-list 111 extended permit icmp host 10.10.10.10 20.20.20.0 255.255.255.0 access-group 111 in interface inside[21]
Linux iptables	-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT -A FORWARD -s 10.10.10.10/32 -p icmp -m icmp --icmp-type any -j ACCEPT -A FORWARD -s 10.10.10.10/32 -p tcp -m tcp --dport 23 -j ACCEPT -A FORWARD -s 10.10.10.10/32 -p tcp -m tcp --dport 80 -j ACCEPT -A FORWARD -s 20.20.20.20/32 -p icmp -m icmp --icmp-type any -j ACCEPT[12]

Table 4. Rules in the firewall for testing

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

### 3.1.3 The limitation in throughput test

One important limitation is the speed of 100Mbps Ethernet port on the Cisco Pagent router. Although the maximum sending rate can be configured more than 4 billion packets per second, the actual output traffic is limited around 100Mbps. To get a reasonable range of the sending rate under this limitation, we do the calculation below:

According to each parameter definitions, the equation is:

$$Traffic(bit/second) = Rate(packet/second) \times Packet\ length(Byte) \times 8bits$$

When the upper bound traffic speed is 100Mbps, we calculate the sending rate individually under two conditions, packet length 1518 bytes and 64 bytes which are the two boundaries in the throughput test, then we get sending the rate is around 8000 to 200,000 packet/s. From this point of view, the maximum sending rate 4 billion packets per second is not actually configured. This figure can be considered as a theoretical value for future usage with supporting hardware. After all Pagent router is a Cisco internal testing equipment not a formal test instrument, there is no any warning indication for unachievable provision data. More details information about this issue is presented in result part.

### 3.2 The implementation of the latency test

The IETF RFC 2544 is still as the main reference of the latency testing process. The traffic used for latency test is different from throughput, it is composed of fixed length packets and these packets were transmitted with a certain rate through the firewall. A normal testing interval is 120 seconds for each data stream. The test was be repeated at least 5 times and then to take the mean value.

Another useful application of the Cisco Pagent router is NQR (Network Quality Reporter) which usually used for a network latency testing. Because NQR can

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

generate the special test traffic with the timestamp and the needed fixed length packets. The timestamp bytes record the latency of the packet traveling through a network. In this experiment, the only network device under test is firewall.

### 3.2.1 Topology of latency test

The topology of latency test is simple. The traffic is sending out of port Fa0/0 on Cisco Pagent router under NQR mode, and then traffic goes through the firewall arriving at the port Fa0/1. NQR is the only test equipment which through analyzing the receiving data that sending by itself to calculate the system latency (Figure 5). In order to get the delay of the firewall products, the system latency with firewall product need to subtract the basic system latency which is not including firewall.

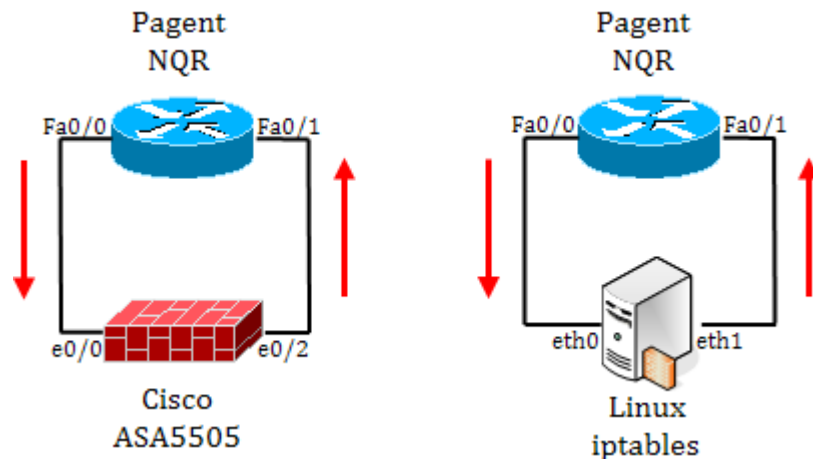


Figure 5. Two kinds of firewall latency test topology

### 3.2.2 The test condition and items in latency test

First, to get the basic system delay, Fa0/0 and Fa0/1 are directly connected by an Ethernet cable, then start the NQR program and record the system latency value without firewalls. One factor needs to be considered is that the cable should have the equal length as the condition with firewall.



## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

Second, the configuration of IP addresses is according to Table 5. The configuration of NQR L2 destination MAC addresses are the same as Table3 in throughput test.

Device	Port	IP address	Subnet mask
Cisco Pagnet NQR	Fa0/0	10.10.10.10	255.255.255.0
Cisco ASA5505	e0/0 (inside)	10.10.10.1	255.255.255.0
Cisco ASA5505	e0/2 (outside)	20.20.20.1	255.255.255.0
Linux iptables	eth0 (inside)	10.10.10.1	255.255.255.0
Linux iptables	eth1 (outside)	20.20.20.1	255.255.255.0
Cisco Pagnet NQR	Fa0/1	20.20.20.20	255.255.255.0

Table 5. IP address table for latency test

The NQR configuration which with the fixed length of packet:

```
rate 1000
length 64,128, 256, 512, 1518
Fastethernet0/0
add tcp
l2-dest 0018.8b83.3d3d
l3-src 10.10.10.10
l3-dest 20.20.20.20
l4-dest 23
Fastethernet0/1 capture[12]
```

### 3.2.3 The limitation in latency test

The Cisco Pagnet router is the most powerful and useful tool in the lab to perform the latency test. However it doesn't provide rich function tools to calculate the latency statistics. The results of test are manually recorded by using the command “show delay-stats” and calculated through subtraction.

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

### 3.3 The implementation of the concurrent sessions test

First, a web server is setup by using Nginx, the homepage is shown as Figure 3. The Webbench works as a client generating a tremendous amount of http requests which form a pressure to the firewall platform. Then the firewall processes these requests and forwards them to the web server. Therefore it reflects the concurrent session capability of firewall. The number of visiting request is increased step by step until the failures appearing in report. Furthermore, the numbers of failure corresponding to the numbers of requests are considered as the performance result.

#### 3.3.1 Topology of concurrent sessions test

The Webbench client generates a huge number of http requests and sends them out of eth0 port. The firewall receives these requests on e0/0, and then forwards them to eth0 port on the web server. At last, the web server receives the requests from the client and replies the requests in order to establish the sessions. (Figure 6)

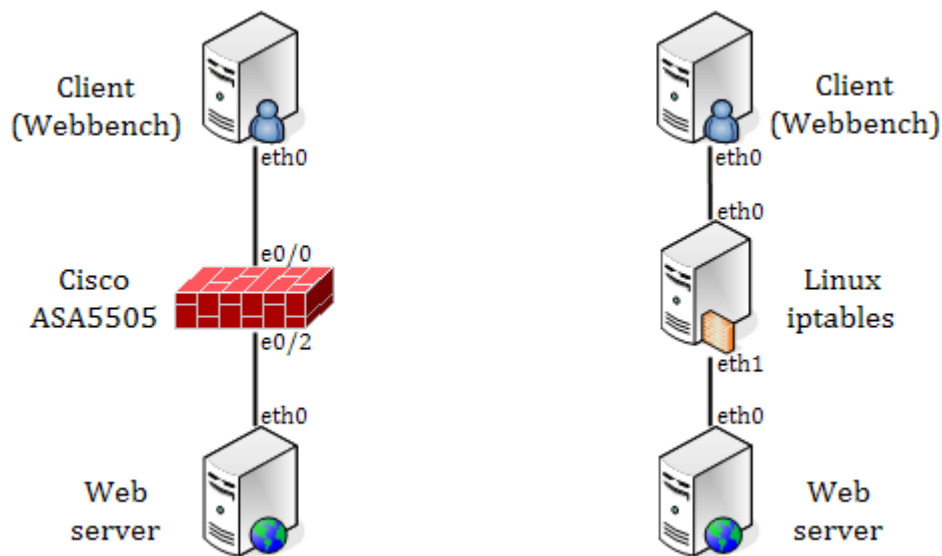


Figure 6. Two kinds of firewall concurrent sessions test topology

#### 3.3.2 The test condition and items in concurrent sessions test

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

The configuration of IP addresses of different devices is according to the list below (Table 6).

Device	Port	IP address	Subnet mask
Client (Webbench)	eth0	10.10.10.10	255.255.255.0
Cisco ASA5505	e0/0 (inside)	10.10.10.1	255.255.255.0
Cisco ASA5505	e0/2 (outside)	20.20.20.1	255.255.255.0
Linux iptables	eth0 (inside)	10.10.10.1	255.255.255.0
Linux iptables	eth1 (outside)	20.20.20.1	255.255.255.0
Web server	eth0	20.20.20.20	255.255.255.0

Table 6. IP address table for concurrent sessions test

After finishing the IP setting, open a browser at the Webbench client and type the link "<http://20.20.20.20/>" to visit the test webpage as Figure 3.

Open a terminal window in Webbench client and type "webbench -c 500 -t 10 <http://20.20.20.20/>" to make a short test to verify the Webbench is working well. It shows thousands number of request succeed and 0 failed, the system is ready for the concurrent session test.

### 3.3.3 The limitation in concurrent sessions test

The Webbench software supports to generate up to 30,000 concurrent sessions. The Nginx web server software supports to establish up to 50,000 concurrent sessions requests. However in this test the main limitation is that the webbench server (DELL laptop LATITUDE D630) can only generate the maximum 15,000 clients requests which depends on its hardware performance.

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

# Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

## 4 Results

The results focus largely on the three mentioned performance parameters from the network layer perspective. Throughput is tested under three types of traffic in order to better understand the algorithms of each firewall. The ntop is the tool to provide the throughput report and the traffic composition. Because there is no tool to perform statistics job, the data of Latency and Concurrent sessions are manually collected and tableted in different forms.

### 4.1 Comparison of throughput results

#### 4.1.1 Fixed packet length under the highest sending rate and burst off setting

Figure 7 and 8 illustrate the last hour throughput results of each firewall under the setting of maximum sending rate (4,294,967,295 packets per second) without burst. However as we discussing in 3.1.3, this figure is not a reasonable value in this test. It is limited by the speed of Ethernet port on traffic generator. According to our throughput results in Table 7 and the equation in 3.1.3, the actually maximum sending rate is around 31,250 packets per second when packet length is 64 bytes. Both of them are taken from the ntop throughput report, and Figure 7 shows the Cisco ASA 5505 and Figure 8 shows Linux iptables firewall. Each green column represents the value of throughput corresponding one type of fixed length packets. The testing interval of each data stream is manually counted about 120 seconds, the next testing starts after another 120 seconds idle time. The details of collected data are shown in Table 7.

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

Packet length (bytes)	Throughput (Mbps)	
	Cisco ASA5505	Linux iptables
64	16	15.1
128	25.8	26.4
256	45.5	45
512	85.1	84.8
1518	94	93.8

Table 7. The max Throughput with the fixed packet length

In both figures, the tendency of throughput value is increasing as the packet length becoming longer. With the same rate setting, the packet length has a significant impact on throughput. In general, the throughput values of both firewalls verify that they belong to the same level. However the Cisco ASA 5505 is a little bit higher than Linux iptables whatever the Max or the Avg values, although the hardware resources of Cisco ASA 5505 are worse than Linux iptables. This difference reflects the algorithm is another factor impacting on the firewall throughput.

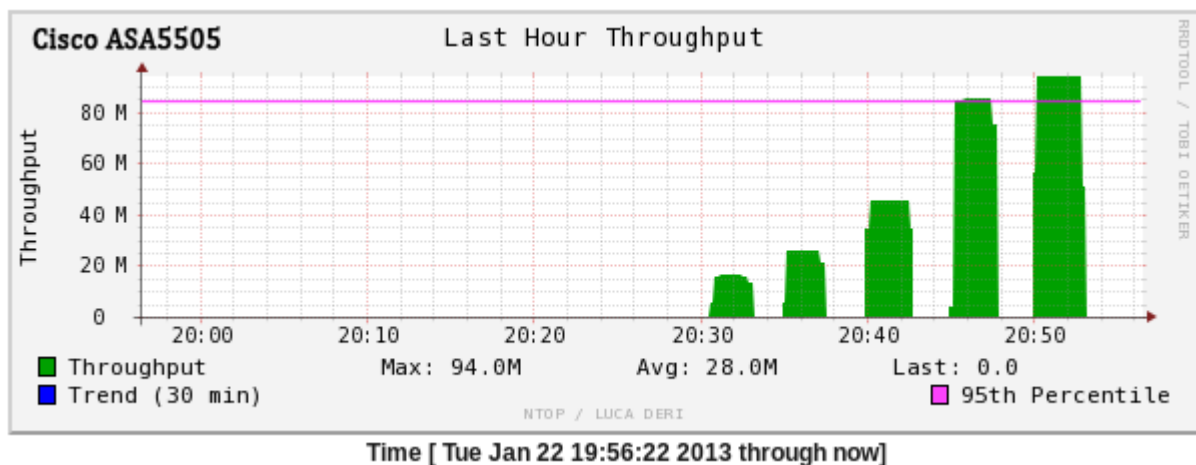


Figure 7. The maximum throughput of Cisco ASA 5505 with different fixed packet length

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

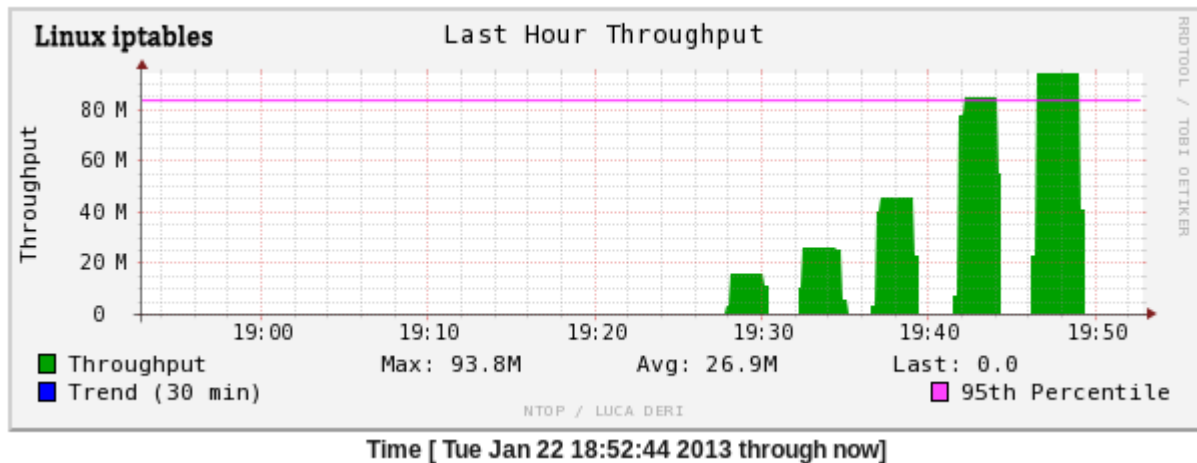


Figure 8. The maximum throughput of Linux iptables with different fixed packet length

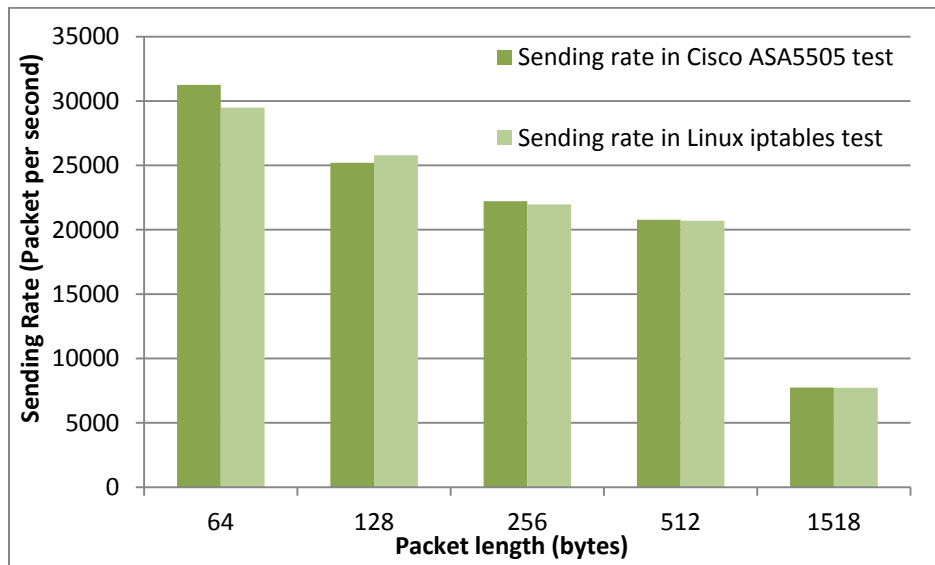


Figure 9. The sending rate versus Packet length

Figure 9 gives a clear view that the sending rate is decreasing as the packet length becomes longer. The actual sending rate is around 8000 to 30,000 packets per second under the limitation 100Mbps of Ethernet port on generator.

### 4.1.2 Random packet length under the different sending rate without burst

In the second throughput test, the test traffic is modified as random packet length (the packet length to be random from 16 bytes to 1500 bytes) under the different sending rate according to Implementation 3.1.2. The main purpose of testing this

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

item is to find which sending rate makes the firewall throughput approaching its maximum level and the behavior of firewall when handling with large amount of continuous traffic. Figure 10 and Figure 11 are the two test report based on the above setting. Cisco ASA 5505 still has a higher throughput than Linux iptables.

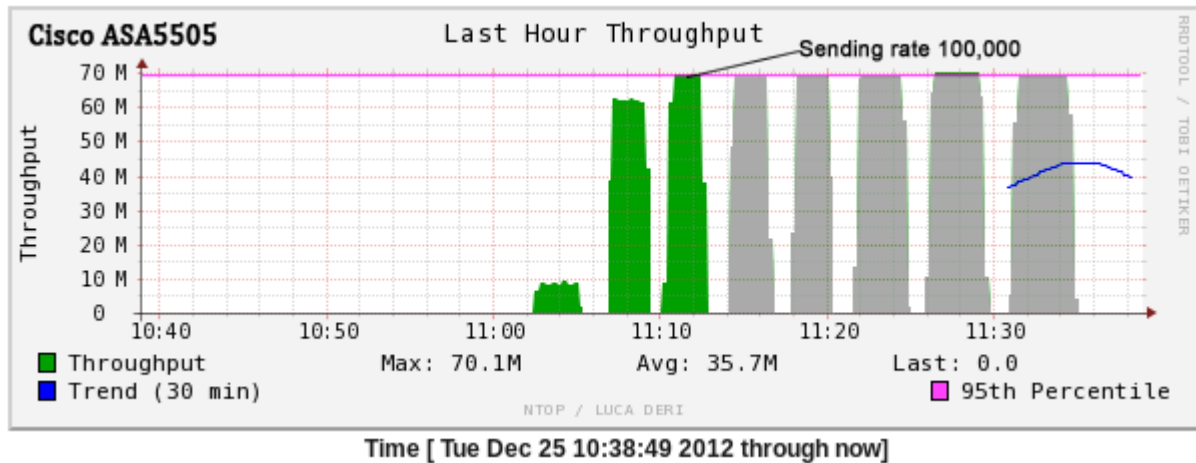


Figure 10. Cisco ASA 5505 throughput with random packet length and different fixed sending rate without burst

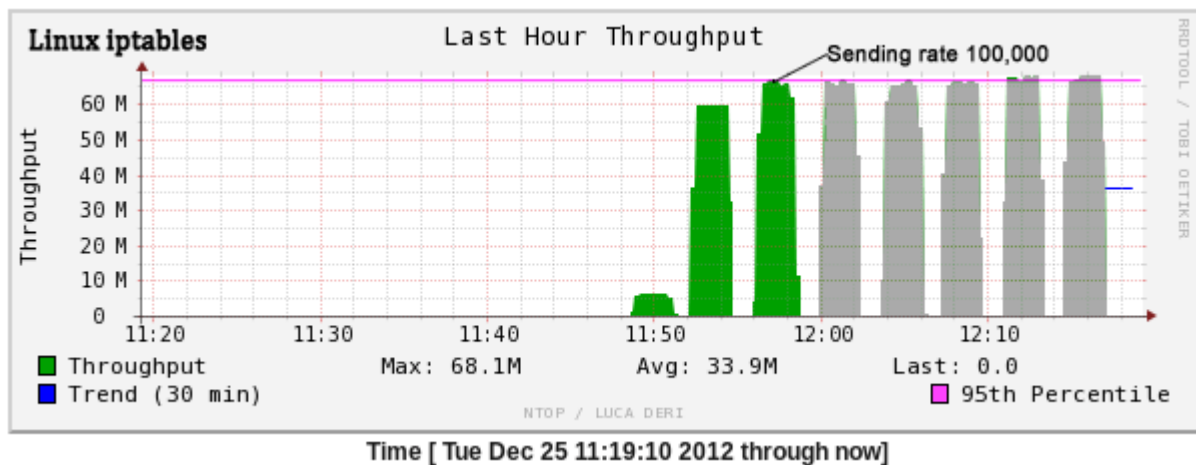


Figure 11. Linux iptables throughput with random packet length and different fixed sending rate without burst

It is different from the last testing report, the variant changes from the different given packet lengths to the different given sending rates. For both figure, there is a



## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

sharp increase nearly 55 Mbits when the sending rate is configured from 1,000 to 10,000. However only about 5 Mbits increment from 10,000 to 100,000, then after 100,000 sending rate, the throughput value gradually stabilize around 70 Mbits. The throughput values after 100,000 sending rate are labeled with grey color manually, because this part of configuration loss of meaning due to the hardware limitation.

Why the throughput value becomes stable above 100,000 sending rate? The reason is that both the Fast Ethernet ports on the Pagent router and on the firewall are 100Mbps. Although the Pagent router has the configuration choice to generate the billion packets per second traffic, it does not mean the rate is fully implemented, because the traffic is limited by the devices' port.

According to the general behavior of network throughput, our initial purpose is to push the throughput of firewall to a peak value and hold on a bit while, then as the sending rate increasing, a clear decrease should appear. However, since the limitation of the lab equipment, it does not come any performance degradation even with the maximum rate setting.

### **4.1.3 Random packet length under the different sending rate with burst**

In the real world, the characteristics of the network traffic are not always smooth and continuous, but intermittent and full filled with burst data. From this point of view, the burst data streams are examined in third throughput test. The test traffic is more approaching to the real traffic on the Internet. The rates above 100,000 are not taken in to consideration as the last.

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

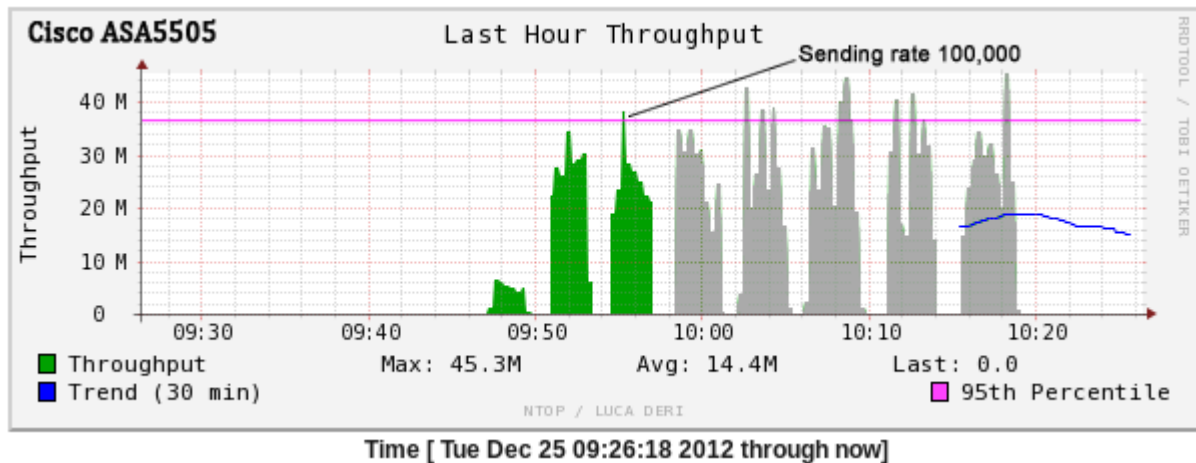


Figure 12. Cisco ASA5505 firewall in burst on state in throughput test

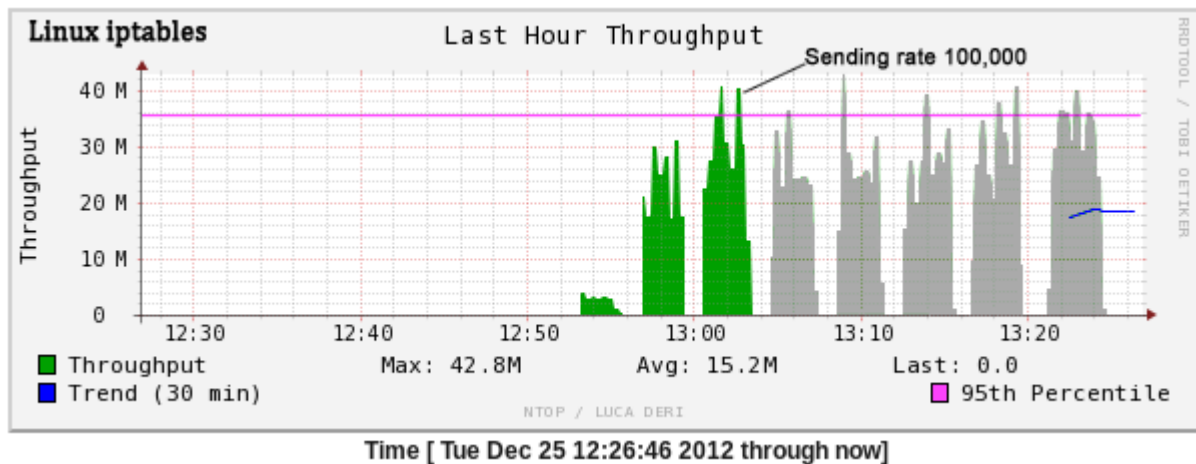


Figure 13. Linux iptables firewall in burst on state in throughput test

Figure 12 and Figure 13 are the results with sending the burst traffic. It is in evidence that the throughput in both figure are becoming uneven. The general increasing tendency is almost the same as last test, but the Max value decreases around 30 Mbits and Avg value gets down nearly 20 Mbits. This indicates that burst traffic obviously impacts on the throughput of firewall. One point is worth mentioning that the Linux iptables Avg 15.2 Mbits is higher than Cisco ASA 5505 14.4 Mbits during this test, but in the other tests it is opposite. Linux iptables firewall has a better ability to handle with burst traffic.

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

### 4.2 Comparison of latency results

Due to the fact that the tested firewalls work on the third layer of OSI model, and the packet forwarding mechanism is using the store-and-forward. Therefore, latency is tested with a given rate and a certain packet length to ensure that the firewall without packet loss. Table 8 is the detailed Average delay with corresponding given packet length. This result is according to the basic configuration in 3.2.2.

Packet length (bytes)	Average delay ( $\mu$ s)	
	Cisco ASA5505	Linux iptables
64	8	19
128	8	19
256	30	58
512	48	75
1518	118	158

Table 8. The average delay in two kinds firewall with different data-length

Note: The name Average delay is a reference from the manual of Cisco Pagent router. It is looked as the latency of the firewall system. In this table, the value is that the firewall system average delay minus the system without firewall. Therefore, this value indicates the delay of firewall.

In Figure 14, the trend chart gives a more clear view of the Average delay going up with the length of given packet becoming larger. The Average delay is described in form of  $\mu$ s and the Packet length is in form of bytes. The sending port and receiving port are directly connected with an Ethernet cable, the length of this cable is almost the same as the cables used for connecting firewall. Linux iptables firewall and Cisco ASA 5505 are represented individually with red and blue color. In evidence, there is no big difference between the two firewalls, but the Cisco ASA 5505 delay is slightly lower than Linux iptables.

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

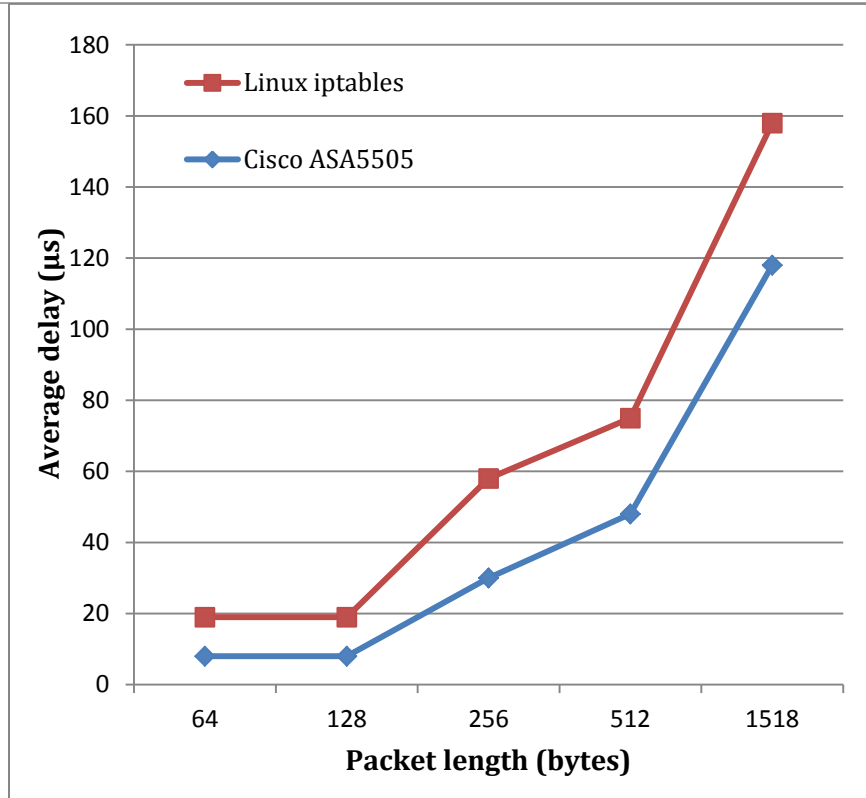


Figure 14. Average delay in latency test

### 4.3 Comparison of concurrent sessions results

The figures in Table 9 display the Concurrent sessions test results. This parameter is tested according the numbers of requesting client which range from 5,000 to 15,000. Every item is tested four times and then calculates the mean value of these results. Finally the Average values are presented in Figure 15.

The numbers of failure request are considered as the monitoring object, to some extent the smaller is the better. The failure is the request which the web server didn't reply to the client. Before this comparison test, a baseline test had been taken. The client server connects to web server directly without firewall. The client server send the 15,000 request and the web bench did not show any failure. Therefore the failure is caused by the firewall.

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

Number of clients	ASA5505 - Number of failures					Linux iptables - Number of failures				
	Test 1	Test 2	Test 3	Test 4	Average	Test 1	Test 2	Test 3	Test 4	Average
5000	0	0	0	0	0.00	0	0	0	0	0.00
6000	0	0	0	0	0.00	0	0	0	0	0.00
7000	0	0	1	0	0.25	0	0	0	0	0.00
8000	0	0	0	2	0.50	0	0	0	0	0.00
9000	0	4	6	21	7.75	0	0	0	0	0.00
10000	0	26	0	3	7.25	0	0	0	0	0.00
11000	0	7	0	91	24.50	0	0	0	0	0.00
12000	0	0	81	177	64.50	0	0	0	0	0.00
13000	410	19	0	0	107.25	0	6	0	0	1.50
14000	15	0	451	21	121.75	27	0	1	0	7.00
15000	0	0	637	13	162.50	4	0	8	0	3.00

Table 9. The test result in two firewall platform with different clients request

The difference between the two firewall products is quite obvious. Before the number of requesting client is below 8,000, the performances of ASA 5505 and iptables are almost the same. Between 8,000 and 10,000, there is seldom failure occurrence. After 10 000 requests, large numbers of failure gradually appear on ASA 5505. It reaches to the highest value 162.5 corresponding to 15,000 requesting clients. However, Linux iptables firewall always keeps a relative low level although with the maximum requests.

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

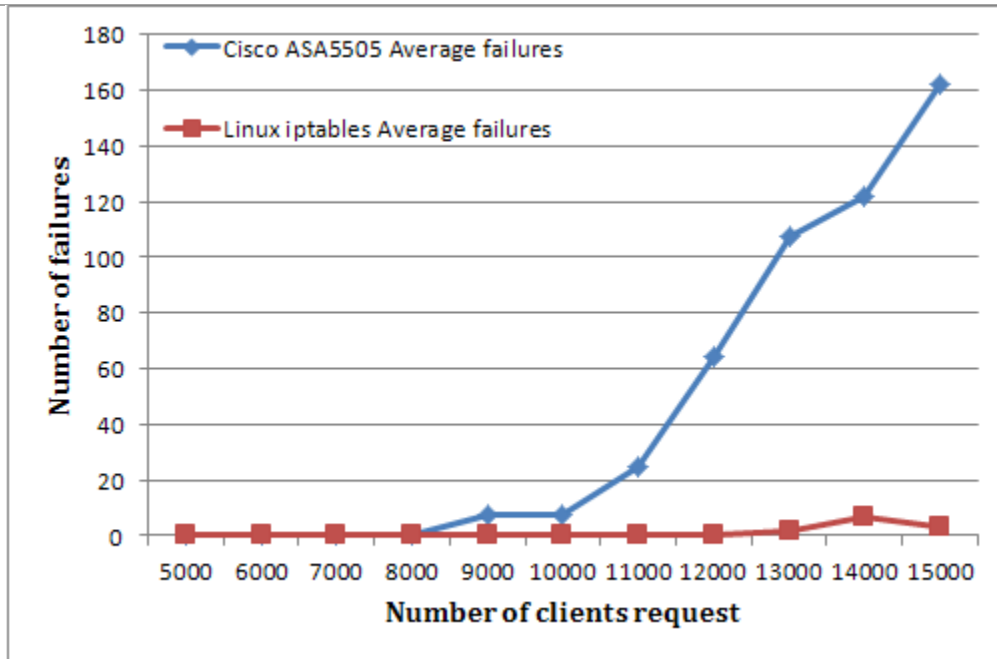


Figure 15. The number of average failures in two firewalls with different clients request

As mentioned in 2.3.3, large numbers of concurrent sessions occupy a big amount of system resources, for example memory and CPU processing power. Figure 16 and Figure 17 display the status of two System Resources separately.

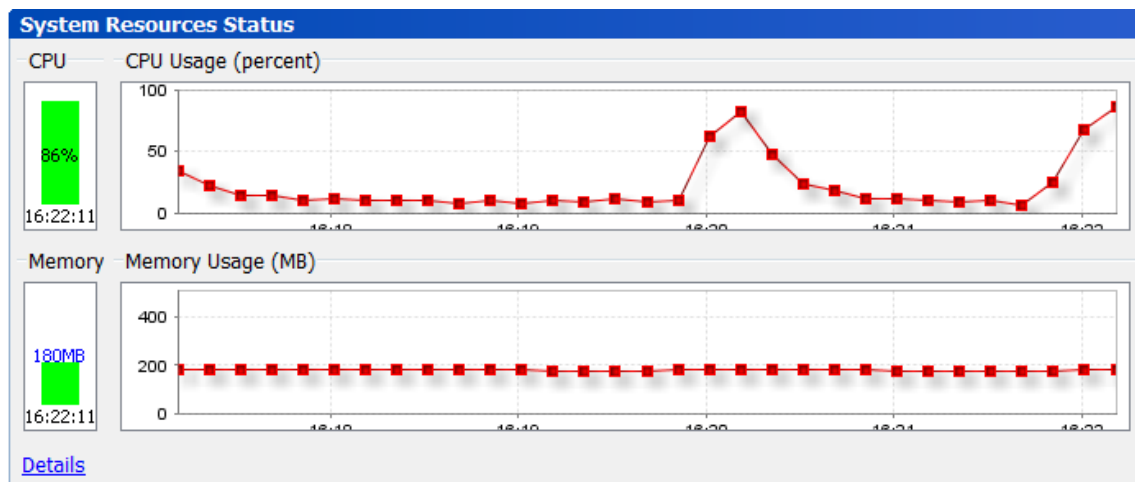


Figure 16. Cisco ASA 5505 system resources status

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

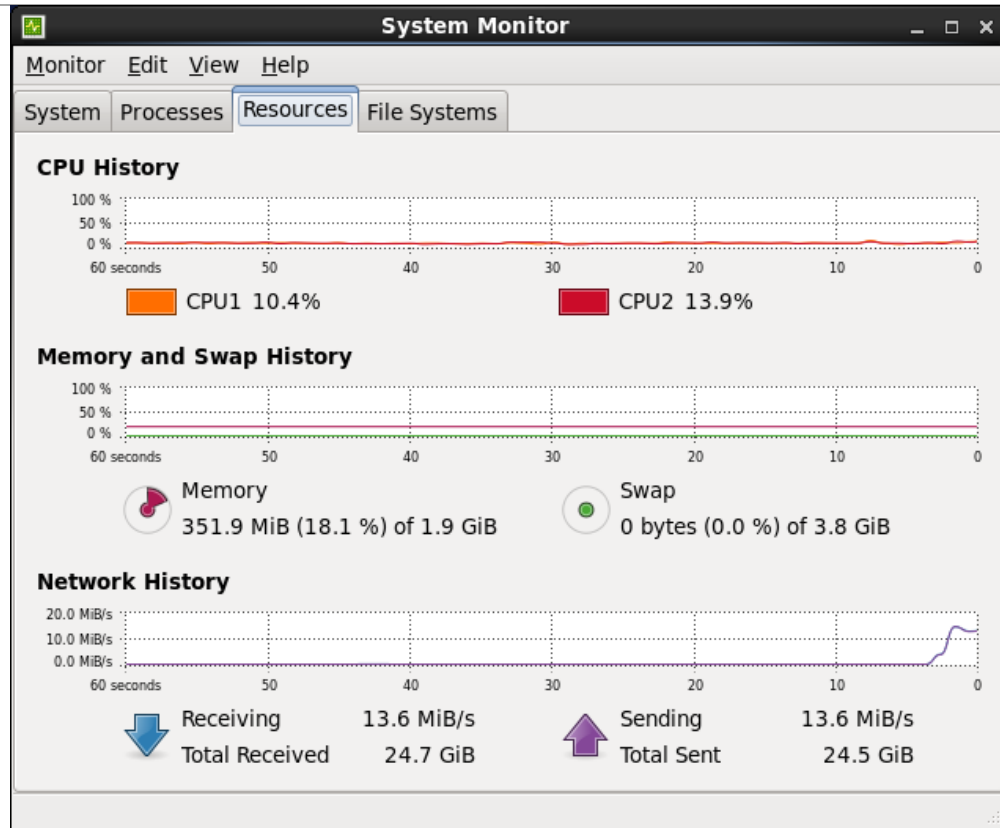


Figure 17. Linux iptables server resources status

Figure 16 is a screenshot of Cisco ASDM for monitoring ASA 5505. Figure 17 is captured from the Linux iptables firewall server. Because the CPU processing speed of iptables is nearly 5 times faster than ASA 5505, in Figure 16 a sharp increment of CPU usage means ASA 5505 is processing large number of requests. However, the CPU of Linux iptables firewall only has very small fluctuations.

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---



## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

### **5 Conclusion**

Two types of firewall, one is hardware-based Cisco ASA 5505 and another is software-based Linux iptables, have been tested individually with three basic network layer performance parameters: Throughput, Latency and Concurrent sessions. Fundamentally, the network performance of a firewall product is not only determined by how advanced the hardware is, but also relies on an optimized algorithm. Both of these two factors play important role in setting up a robust firewall system.

According to the test result, each firewall has its own advantages, but they can be categorized in the same class. Under the throughput and the latency test, the performance of Cisco ASA 5505 is better than Linux iptables although the latter equipped with more advanced hardware, but the differences are not great. It reflects ASA 5505 has a more optimized algorithm. The Linux iptables firewall has a stronger ability of handling burst traffic and large number of concurrent session requests, it could attribute the success to higher hardware equipment.

From other point of view, ASA 5505 is an exclusive firewall product providing more interfaces access and smaller size; it is much easier to be deployed under industrial conditions. However the cost is more expensive than an equivalent Linux iptables firewall product, in addition, ASA 5505 still requires another computer as a terminal to perform management. Iptables firewall solution is integrated in the Linux operation system which has become extremely popular in the IT industry because of its robustness, reliability, flexibility, and seemingly unlimited scope for customization. The high degree of flexibility and open also makes the maintenance work complex which usually needs the operator having strong background of Linux knowledge. In one word, Cisco ASA 5505 is suitable for a small or medium enterprise. Linux iptables is a very good firewall solution for the private or a small group who are enthusiasts of Linux system. Of course, it can be deployed in a company, one practical consideration is maintenance.

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

The evaluation of a firewall system includes many aspects depending on special requirements. Based on the limited resources, this thesis is only focusing on network layer parameters test. In reality, the security, functionality and management of a firewall are also in the scope of evaluation. In spite of how to choose a right firewall product is always a stressful problem, a detailed requirement list with priority is the key to solve it. The next is to avoid some misunderstandings of different parameters. The test data from lab or the manual can only be used as a basic reference, because in reality when a firewall is deployed for an enterprise, it's impossible to use only one function. When all the functions are enabled, the performance of that certain aspect will be much lower than it's indicated in the manual.

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

### Reference

- [1] Thakar, U., Purohit, L., & Pahade, A. (2012, September). An approach to improve performance of a packet-filtering firewall. In *Wireless and Optical Communications Networks (WOCN), 2012 Ninth International Conference on* (pp. 1-5). IEEE.
- [2] Bradner, S. (1991). RFC 1242. *Benchmarking Terminology for Network Interconnection Devices*, "Harvard University.
- [3] Bolla, R., & Bruschi, R. (2006). RFC 2544 performance evaluation and internal measurements for a Linux based open router. In *High Performance Switching and Routing, 2006 Workshop on* (pp. 6-pp). IEEE.
- [4] Sheth, C., & Thakker, R. (2011, February). Performance Evaluation and Comparative Analysis of Network Firewalls. In *Devices and Communications (ICDeCom), 2011 International Conference on* (pp. 1-5). IEEE.
- [5] Newman, D. (1999). RFC 2647: Benchmarking terminology for firewall performance. *Network Working Group, Internet Engineering Task Force (IETF)*.
- [6] Komar, B., Beekelaar, R., & Wettern, J. (2003). *Firewalls for dummies*. For Dummies.
- [7] Zwicky, E., Cooper, S., & Chapman, D. (2000). *Building internet firewalls*. O'Reilly Media, Incorporated.
- [8] Packet Filtering, InfoSec Institute Resources. URL: <http://resources.infosecinstitute.com/packet-filtering/> (Last accessed: January 21, 2013).
- [9] Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). *Firewalls and Internet security: repelling the wily hacker*. Addison-Wesley Professional.
- [10] Firewalls, Tech-FAQ. URL: <http://www.tech-faq.com/firewall.html> (Last accessed: January 21, 2013).

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

- [11] Cisco Systems Inc., Cisco ASA 5500 Series Security Appliances URL: [http://www.cisco.com/en/US/products/ps6120/prod\\_models\\_comparison.html](http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html) (Last accessed: January 21, 2013).
- [12] CentOS, HowTos Network IPTables. URL: <http://wiki.centos.org/HowTos/Network/IPTables> (Last accessed: January 15, 2013).
- [13] ntop, product overview. URL: <http://www.ntop.org/products/ntop/> (Last accessed: January 21, 2013).
- [14] Cisco Systems Inc., Cisco Adaptive Security Device Manager. URL: <http://www.cisco.com/en/US/products/ps6121/index.html> (Last accessed: January 21, 2013).
- [15] Ciscoconsole, TGN Traffic Generation Using Cisco Pagent IOS. <http://www.ciscoconsole.com/nms/traffic-generation-using-cisco-pagent-ios.html/> (Last accessed: January 21, 2013).
- [16] Cisco Systems Inc., TGN (Traffic GeNerator)User Manual. tgn.pdf
- [17] Cisco Systems Inc., NQR (Network Quality Reporter)User Manual. nqr.pdf
- [18] Nginx, wiki main. URL: <http://wiki.nginx.org/Main> (Last accessed: January 21, 2013).
- [19] Nginx: the High-Performance Web Server and Reverse Proxy, Linux Journal. URL: <http://www.linuxjournal.com/magazine/nginx-high-performance-web-server-and-reverse-proxy?page=0.0> (Last accessed: January 21, 2013).
- [20] Web bench homepage, webbench 1.5. URL: <http://home.tiscali.cz/cz210552/webbench.html> (Last accessed: January 21, 2013).
- [21] Cisco Systems Inc., Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2. <http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/config.html> (Last accessed: December 24, 2012).

## **Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions**

---

# Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

## Appendix

### 1. Cisco Pagent TGN configuration:

TrafGen(TGN:OFF,Fa0/0:2/2)#sh

Traffic stream 2 of 2, TCP, FastEthernet0/0 (up)

name ""

on

rate 1000

variability 0

send 0

repeat 1 no-update

delayed-start random

burst on

burst duration on 1000 to 10000

burst duration off 5000 to 10000

!

datalink user-defined

fragmentation disable

length random 60 to 1500

!

L2-encapsulation arpa

L2-dest-addr 0018.8B83.3D3D

L2-src-addr 0017.E049.B7E0

L2-protocol 0x0800

!

L3-version 4

L3-header-length auto

L3-tos 0x00

L3-length auto

L3-id 0x0000

L3-fragmentation 0x0000

L3-ttl 60

L3-protocol 6

L3-checksum auto

L3-src-addr 10.10.10.10

L3-dest-addr 20.20.20.20

L3-option-length 0

!

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

```
L4-src-port 0
L4-dest-port 80
L4-sequence 0x00000000
L4-acknowledge 0x00000000
L4-header-length auto
L4-flags 0x00
L4-window 0
L4-checksum auto
L4-urgent 0
L4-option-length 0
!
data-length 26
!      0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
data 0 "47 45 54 20 2F 69 6E 64 65 78 2E 68 74 6D 6C 20 48 54 54 50"
data 20 "2F 31 2E 31 20 20"
!
fill-pattern 0x00 0x01
!
isl-crc-added off
```

### 2. Cisco Pagent NQR configuration:

```
TrafGen(NQR:OFF,Fa0/0:1/1)#sh
```

```
Traffic stream 1 of 1, TCP, FastEthernet0/0 (up)
name ""
on
rate 1000
variability 0
send 0
convg-buffer-size 2000
repeat 1 no-update
receive-mode unicast
delayed-start random
burst off
burst duration on 1000 to 1000
burst duration off 1000 to 1000
!
datalink user-defined
```



## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

```
length 64
!
L2-encapsulation arpa
L2-dest-addr 0018.8B83.3D3D
L2-src-addr 0017.E049.B7E0
L2-protocol 0x0800
!
L3-version 4
L3-header-length auto
L3-tos 0x00
L3-length auto
L3-id 0x0000
L3-fragmentation 0x0000
L3-ttl 60
L3-protocol 6
L3-checksum auto
L3-src-addr 10.10.10.10
L3-dest-addr 20.20.20.20
L3-option-length 0
!
L4-src-port 0
L4-dest-port 23
L4-sequence 0x00000000
L4-acknowledge 0x00000000
L4-header-length auto
L4-flags 0x00
L4-window 0
L4-checksum auto
L4-urgent 0
L4-option-length 0
!
data-length 26
!      0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
data 0 "00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00"
data 20 "00 00 00 00 00 00"
!
fill-pattern 0x00 0x01
!
isl-crc-added off
```

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

### 3. Cisco ASA5505 firewall configuration:

```
ASA5505# sh run
: Saved
:
ASA Version 8.2(5)
!
hostname ASA5505
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 switchport access vlan 10
!
interface Ethernet0/1
 shutdown
!
interface Ethernet0/2
 switchport access vlan 20
!
interface Ethernet0/3
 shutdown
!
interface Ethernet0/4
 shutdown
!
interface Ethernet0/5
 shutdown
!
interface Ethernet0/6
 shutdown
!
interface Ethernet0/7
 switchport access vlan 99
!
interface Vlan1
 no nameif
```

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

```
no security-level
no ip address
!
interface Vlan10
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
interface Vlan20
 nameif outside
 security-level 0
 ip address 20.20.20.1 255.255.255.0
!
interface Vlan99
 nameif management
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!
ftp mode passive
access-list 111 extended permit tcp host 10.10.10.10 host 20.20.20.20 eq www
access-list 111 extended permit tcp host 10.10.10.10 host 20.20.20.20 eq telnet
access-list 111 extended permit icmp host 10.10.10.10 20.20.20.0 255.255.255.0
pager lines 24
mtu inside 1500
mtu outside 1500
mtu management 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
access-group 111 in interface inside
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
```

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

```
http server enable
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0

threat-detection basic-threat
threat-detection statistics access-list
threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400 average-rate
200
webvpn
  anyconnect-essentials
  username cisco password 3USUcOPFUiMCO4Jk encrypted
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
```

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

```
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:9e98da5f7ccd1bb7a92b95e9ca7f9562
: end
```

### 4. Linux iptables firewall configuration:

```
# Generated by iptables-save v1.4.7 on Sun Jan 26 22:01:00 2003
*nat
:PREROUTING ACCEPT [2213:180877]
:POSTROUTING ACCEPT [36:2667]
:OUTPUT ACCEPT [31:2167]
COMMIT
# Completed on Sun Jan 26 22:01:00 2003
# Generated by iptables-save v1.4.7 on Sun Jan 26 22:01:00 2003
*filter
:INPUT ACCEPT [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

```
-A FORWARD -s 10.10.10.10/32 -p icmp -m icmp --icmp-type any -j ACCEPT
-A FORWARD -s 10.10.10.10/32 -p tcp -m tcp --dport 23 -j ACCEPT
-A FORWARD -s 10.10.10.10/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A FORWARD -s 20.20.20.20/32 -p icmp -m icmp --icmp-type any -j ACCEPT
COMMIT
# Completed on Sun Jan 26 22:01:00 2003
```

### 5. Cisco Pagent router configuration:

TrafGen#sh run

Building configuration...

Current configuration : 992 bytes

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname TrafGen
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
!
!
ip cef
!
!
ip host PAGENT-SECURITY-V3 97.32.43.85 87.84.0.0
!
multilink bundle-name authenticated
!
!
voice-card 0
no dspfarm
```

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

```
!  
buffers huge size 65820  
!  
interface FastEthernet0/0  
ip address 10.10.10.10 255.255.255.0  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
ip address 20.20.20.20 255.255.255.0  
duplex auto  
speed auto  
!  
interface Serial0/0/0  
no ip address  
shutdown  
no fair-queue  
clock rate 2000000  
!  
interface Serial0/0/1  
no ip address  
shutdown  
clock rate 2000000  
!  
ip route 0.0.0.0 0.0.0.0 10.10.10.1  
!  
ip http server  
no ip http secure-server  
!  
control-plane  
!  
line con 0  
exec-timeout 0 0  
line aux 0  
line vty 0 4  
login  
!  
scheduler allocate 20000 1000  
!
```

## Performance Evaluations of Cisco ASA and Linux iptables Firewall Solutions

---

end

### 6. Linux iptables status:

[root@localhost Desktop]# service iptables status

Table: filter

Chain INPUT (policy ACCEPT)

num	target	prot	opt	source	destination
-----	--------	------	-----	--------	-------------

Chain FORWARD (policy DROP)

num	target	prot	opt	source	destination
-----	--------	------	-----	--------	-------------

1	ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	state
---	--------	-----	----	-----------	-----------	-------

RELATED,ESTABLISHED

2	ACCEPT	icmp	--	10.10.10.10	0.0.0.0/0	icmp type 255
---	--------	------	----	-------------	-----------	---------------

3	ACCEPT	tcp	--	10.10.10.10	0.0.0.0/0	tcp dpt:23
---	--------	-----	----	-------------	-----------	------------

4	ACCEPT	tcp	--	10.10.10.10	0.0.0.0/0	tcp dpt:80
---	--------	-----	----	-------------	-----------	------------

5	ACCEPT	icmp	--	20.20.20.20	0.0.0.0/0	icmp type 255
---	--------	------	----	-------------	-----------	---------------

Chain OUTPUT (policy ACCEPT)

num	target	prot	opt	source	destination
-----	--------	------	-----	--------	-------------

Table: nat

Chain PREROUTING (policy ACCEPT)

num	target	prot	opt	source	destination
-----	--------	------	-----	--------	-------------

Chain POSTROUTING (policy ACCEPT)

num	target	prot	opt	source	destination
-----	--------	------	-----	--------	-------------

Chain OUTPUT (policy ACCEPT)

num	target	prot	opt	source	destination
-----	--------	------	-----	--------	-------------



