WHITE PAPER

April 1997

Prepared By
Intranet/Groupware
Solutions Group

Compaq Computer
Corporation

Performance Analysis and Tuning of Raptor's Eagle NT 3.06 Firewall on Compaq Servers

As firewalls make their mark as a security measure used to protect intranetworks, it is not clear what is lost from network performance when security is implemented. Today, the lack of multi-protocol benchmark tools makes it difficult to determine network performance through firewalls. Since few tools are available and most are used to determine http performance, determining the loss of network performance and what can be done to improve it remains difficult.

This paper looks at performance of firewalls using Raptor's Eagle NT 3.06 product on Compaq servers, and the popular protocols ftp and http. It answers questions about the level of hardware needed to address capacity planning, software tuning parameters for the system and firewall, and what to expect in performance gains and losses while incorporating a secure environment for internet connections.

CONTENTS

COMPAQ

NOTICE

The information in this publication is subject to change without notice.

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

This publication does not constitute an endorsement of the product or products that were tested. The configuration or configurations tested or described may or may not be the only available solution. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state or local requirements. Compaq does not warrant products other than its own strictly as stated in Compaq product warranties.

Compaq, ProLiant, and SmartStart, registered United States Patent and Trademark Office.

Netelligent and ProSignia are trademarks and/or service marks of Compaq Computer Corporation.

Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Microsoft, Windows, Windows NT, Windows NT Advanced Server, SQL Server for Windows NT are trademarks and/or registered trademarks of Microsoft Corporation.

Eagle, Eagle NT 3.06, and Raptor are trademarks and/or registered trademarks of Raptor Systems Inc.

NSTL makes no recommendations or endorsement of any product. This data was prepared by the client using licensed testing products from NSTL. NSTL does not guarantee the accuracy, adequacy, or completeness of the services provided in the connection with the clients product. NSTL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO RESULTS TO BE ONTAINED BY ANY PERSON OR ENTITY FROM USE OF THE SERVICES OR THE RESULTS THEREOF, OR ANY INFORMATION OR DATA INCLUDED THEREIN NSTL MAKES NO EXPRESSED OR IMPLIED WARRANTIES OR MERCHANTABILITY OR FIRNESS FOR A PARTICULARPURPOSE OR USE WITH RESPECT TO THE SERVICES AND/OR RESULTS TEREROF, OR ANY INFORMATION OR DATA INCLUDED THEREIN.

Firewall Performance Tuning
First Edition (April 1997)
278A/0497

INTRODUCTION

The intent of this paper is to help answer questions about performance of firewalls so that logical decisions can be made for capacity planning using Raptor's Eagle NT 3.06 firewall product. A base line for a specified firewall system is defined, options are added to the base line, and the load differences and performance are evaluated. This base line is used to determine how each configuration change affects the performance of the firewall from the base line system.

This paper starts by describing different benchmarks available, gives a definition of the methodology chosen for the tests and the test bed setup, describes the rationale for determining performance characteristics used in the test, explains test cases based on the characteristics, and evaluates the results.

EXECUTIVE SUMMARY

This paper uses the NSTL software benchmark methodology to test firewall performance on the Eagle NT 3.06 firewall. A base line test is run and individual hardware and software components are added to the base system and the differences are evaluated. Variable hardware and software components modified in the tests include memory, bus architecture, drive controller, network speed, Raptor's Eagle NT 3.06 HTTP Cache and DNS Lookup switches, the firewall rule base with 100 rules, and NetFlx-3 MaxRecieve buffers.

From the sets of test run, the following performance summary resulted:

- For hardware configurable tests, upgrading the Network Interface Cards from the EISA bus to the PCI bus achieved very noticeable increases in performance.
- The processor scales well with two processors, making dramatic increases in performance as the load increases.
- Adding memory increases performance slightly as the load increases.
- Network throughput also increased when changed from a 10Mb network to 100Mb network. The firewall was able to process more than 10Mb worth of data through the firewall with both HTTP/FTP and HTTP only transactions, with large loads, and showed expected decreases with normal loads on a 10 Mb network because of higher collision rates.
- Software configurable tests with HTTP Cache on, resulted in increased performance in both HTTP/FTP and HTTP only tests.
- Tests with the DNS Lookups for HTTP switch turned off, displayed high performance increases for greater loads on HTTP Only tests.
- Differences between HTTP/FTP and HTTP only transfers showed increased results for HTTP only transfers, highlighting the added performance enhancements included in Raptor's Eagle NT 3.06 firewall product for HTTP.

BENCHMARK TOOLS

The popular benchmarking tools available today are used to test webserver or system performance only. Webserver benchmarks can generate loads for static web pages of varying sizes, test webserver processor performance using CGI or ISAPI/NSAPI loads, and calculate the transaction times, throughput, and connections per second. Most benchmarks use a control station for gathering and reporting load data and starting virtual client sessions. Although these benchmarks determine performance and load capacity for webservers, they do not exercise the variability of multi-protocol loads through gateways/firewalls. Multi-protocol benchmarks allow firewalls to be stressed in ways, which closely simulate real network traffic. Of the four benchmarks described below, NSTL's Benchmark enables two protocols to be used, HTTP and FTP, which are the two most used on the Internet and thus the tool used to test performance of the firewall in this paper.

WebStone

Webstone measures the raw throughput of a standard HTTP workload. It is measured across two main variables--latency, in seconds, and the number of connections per second. Other data can also be collected, such as throughput in bits per second. The benchmark itself uses a client/server architecture, and each client runs a configuration file that tells it which server to connect to, how long to maintain the connection, and which URLs to fetch.

WebBench

WebBench reports two types of results: the average number of requests per second the HTTP server handled, and the average number of bytes per second that moved between the clients and the server. The controller computes these results by collecting each client's results as that client finishes the test.

SpecWeb

SpecWeb measures the response time for server requests across a number of different workloads. It sends HTTP requests to the server, based on defined workload parameters, and calculates the overall throughput at the end of a run. The workload information that the benchmark takes into account includes request rate and request type, file set, database transactions, security, and slow networks.

NSTL Benchmark

This benchmark was designed specifically to stresses the ability of the firewall to route traffic based on a set of rules. It simulates real usage of the firewall by directing heavy loads of FTP and HTTP traffic through the firewall. The toolkit also allows WAIS traffic and CGI requests to be sent. The results are measured in overall transaction time for each client data transfer for a set of virtual clients. This is then broken down into TPM (Transactions per Minute) based on the number of URLs and FTP files requested.

NSTL METHODOLOGY OF INTERNET FIREWALLS

This section describes in detail the NSTL methodology used for the tests and the alterations made to the methodology to allow more traffic to pass through the firewall.

Configuration

The NSTL methodology was designed to stress the ability of the firewall to route traffic based on a set of rules. Heavy loads of HTTP and FTP traffic are generated for requests through the firewall. The overall transaction time for each client transfer is measured and reported under various load conditions. The original methodology used three scenarios for measuring performance through the firewall. Together, the three scenarios did not provide an effective challenge to the firewall, so changes were made to NSTL's benchmark configuration to allow more traffic to pass through the firewall from both sides.

Transaction refers to the amount of time it takes to open a connection from the client to the server, request data from the server, download that data from the server to the client, and closing the connection from the client to the server. Transactions are measured in Transactions Per Minute. (TPM)

This scenario, described in more detail below, is the scenario used in the benchmark tests for this paper. Performance ratings for the test runs are calculated from individual performance scores for the number of virtual clients used in the tests. Performance ratings are then translated into transactions per minute. This rating reflects the speed at which the firewall system processes network traffic, as it performs security tasks based on the security rule set.

The security model that the NSTL Methodology uses specifies security zones, security rules, the protocols used in each security rule set, and logging. The benchmark creates load through the firewall by establishing multiple virtual clients on each physical client machine in each security zone. A control client is used to send requests to each physical client that dictates the number of virtual clients it used and gathers, from the virtual clients, the transaction information used to calculate the transactions per minute. (See Figure 1)

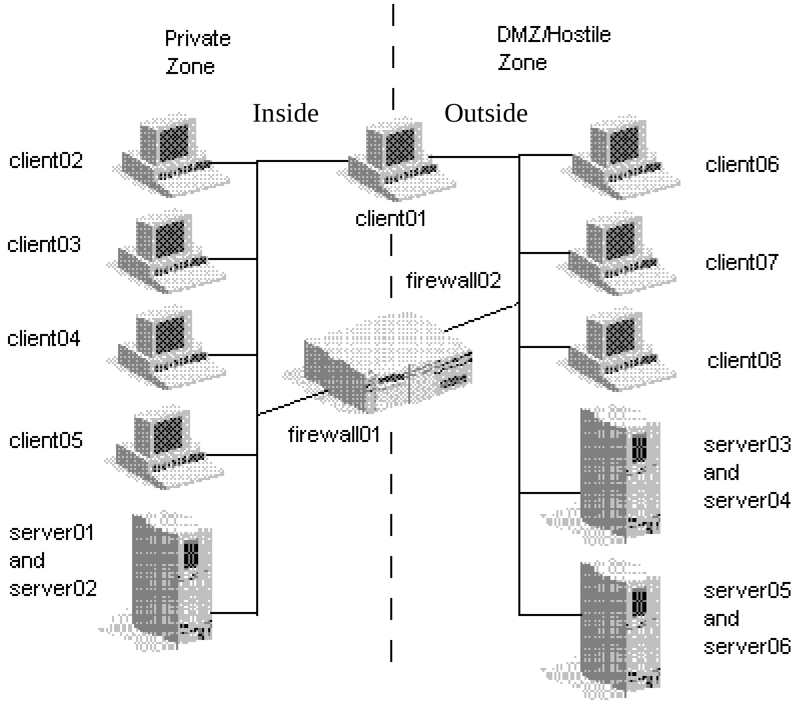


Figure 1: **Test Bed Configuration**

Three areas determine security zones:

- **Private Zone -** the secure area of the network or the area protected from the Internet with a firewall. Internal networks reside in the private area.
- **DMZ -** the network area unsecured by the firewall. Usually Internet servers are located here such as Web Servers, News Servers, DNS Servers, FTP Servers, etc.
- **Hostile Zone -** or public area, is the cloud of the Internet or the outside network.

NSTL's benchmark can be run with the three zones implementing three network segments or with two network segments. When two network segments are used, the DMZ and the Hostile Zone are combined. This is the setup selected for performance evaluation of Raptor's Eagle NT 3.06 contained in this paper.

The security rule set contains the following rules using FTP ports (20,21), HTTP port (80) protocols:

- **Private to Private, Private to Hostile, and Private to DMZ -** Allow All
- **Hostile/DMZ to Private -** Allow only to specified servers.

Logging affects the firewall throughput; therefore moderate logging is used. This logs all connections, spoof detection messages, TCP syn/fin messages, and connect rejection messages.

The test methodology uses 6 virtual servers from 3 physical servers and 1 to 72 virtual clients on 8 physical clients. Virtual clients are administered from one of the physical clients known as the control machine. Each virtual client makes 100 request for FTP GET and HTTP GET transfers to the 6 virtual servers. HTTP/CGI requests were also available but not used because HTTP/CGI requests could skew the totals due to web server processing of CGI requests.

Percentages used to determine the amount of traffic the virtual clients send to the virtual servers is a configurable item for the methodology. For configurations used in test runs contained in this paper, each virtual server receives the percentages of HTTP and FTP requests from the virtual clients as listed in Table 1.

Servers	% FTP requests	% HTTP requests
server01, server03, server05	10	90
server02, server04, server06	90	10

Table 1: **Test Bed Protocol Percentage**

Server requests percentages are the same for all sets of virtual clients used. Also, the setup places server01 and server02 in the Private Zone and server03 through server06 in the DMZ/Hostile Zone. This setup follows the procedures used in previous NSTL tests.

The amount of requests per virtual client is also configurable. In practice, using 100 requests per virtual client and using up to 72 virtual clients produces a good load on the client systems and pushes a high amount of traffic through the network. Therefore, using 72 virtual clients was adopted as the maximum number of virtual clients used in the test runs. In all test runs (eight per hardware configuration), the number of virtual clients was 1, 12, 24, 32, 36, 48, 60, and 72. This approach in the number of virtual clients used shows how the firewall reacts under progressively heavier loads. The percentages of servers that are hit from each of the physical clients are also configurable items as presented in Table 2.

Clients	server01	server02	server03	server04	Server05	server06
client01 - client05	2.4%	2.4%	23.8%	23.8%	23.8%	23.8%
client06 - client08	40%	40%	5%	5%	5%	5%

Table 2: **Percentage of Servers hit by Clients**

The file types used for transactions for the benchmark were ZIP files for FTP transfers and HTML and GIF files for HTTP transactions. The sizes of the files for FTP are 32, 64, 128, and 256 kilobytes. HTTP file sizes, with one directory depth, were 1, 2, 4, 8, 10, 20, 40, and 80 kilobytes for HTML files and 512 bytes, 1, 2, 4, 10, 26, 52, 104, and 208 kilobytes for GIF files. All files were automatically generated using the NSTL configuration toolkit.

Using NSTL's two-zone configuration (private zone behind the firewall and DMZ and hostile zone in front of the firewall), two physical servers are located in the DMZ/hostile zone and one physical server is located in the private zone. Physical client configurations place the control station between the two network segments (client01), four clients in the private zone (client02 through client05), and three clients in the DMZ/hostile zone (client06 through client08). Having the control station between both network segments allows data to flow across both networks with no interaction with the firewall, thus simulating real FTP and HTTP network traffic. Also, the control station is used to gather transaction time information and send virtual client load information to the physical clients on port (2001). Please refer to Figure 1 for a pictorial view of the testbed.

Test Bed Setup

Table 3 describes the hardware and software for the clients and web servers used in the test bed setup. All clients and servers are connected to a 100Mb network except for one test set, which connects clients and servers to a 10Mb network. Network configurations are discussed in the section Hardware and Software Tuning Characteristics.

Machine	Hardware	OS	Software
Client01	ProLiant 2000, 2-Pentium/90, 64 MB RAM, 2 EISA NetFlx-3 10/100 NIC, ON BOARD SCSI, 2 GB Drive	Windows NT 4.0 Workstation, Service Pack 2	NSTL Firewall Benchmark Software for client machines, NSTL controller software
client02 - client08	ProLiant 2000, 2-Pentium/90, 32 MB RAM, 1 EISA NetFlx-3 10/100 NIC, ON BOARD SCSI, 2 GB Drive	Windows NT 4.0 Workstation, Service Pack 2	NSTL Firewall Benchmark Software for client machines
server01 - server06	ProLiant 2000, 2-Pentium/90, 32 MB RAM, 1 EISA NetFlx-3 10/100 NIC, ON BOARD SCSI, 2 GB Drive	Windows NT 4.0 Server, Service Pack2	Microsoft IIS 3.0 configured with FTP and HTTP

Table 3: **Client and Server Hardware Makeup**

Eagle NT 3.06 Firewall Setup of Base System

The hardware and software setup for Raptor's Eagle NT 3.06 firewall starts with a base system configuration. Modifications are made to hardware and software on the firewall to determine performance differences from the base system. Determinations can be made at this point about how the firewall handles different configurations. An explanation about differences in the configurations and the reasons why such configurations were chosen are discussed in the section Hardware and Software Tuning Characteristics.

This section discusses the hardware and software requirements for a base system configuration. It also shows the configuration of the Raptor Eagle NT 3.06 firewall using the GUI to the firewall (Hawk) and concentrates on the configuration items that do not change for all test runs.

Table 4 shows the hardware and software makeup of the firewall for the base system.

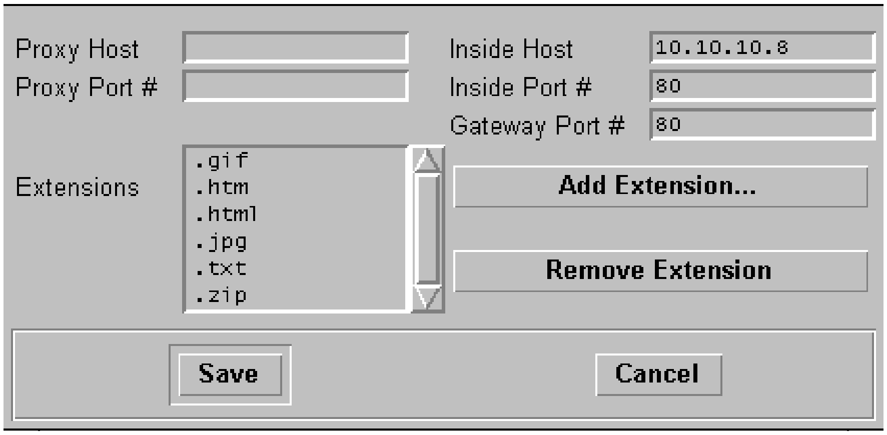
Machine	Hardware	OS	Software
firewall01	ProLiant 5000, 64 MB RAM, 1-Pentium PRO 200/512K cache, 2 EISA NetFlx-3 10/100 NICs, PCI-Smart-2 Ctrl, 1-2 GB Drive	Windows NT 3.51 Server, Service Pack 5	Raptor's Eagle NT 3.06 firewall software and Hawk GUI.

Table 4: **Firewall Hardware and Software Makeup**

Firewall configuration with Eagle NT 3.06 starts with DNS setup. The network segments for Inside and Outside used the network addresses `10.10.10` and `11.11.11` respectively and the domain was set to `testbed.com` for both segments. This information was configured from the **`Gateway`** screen `File->Set up DNS... menu option.`

Two files: HOSTS and HOSTS.PUB located in the `%SYSTEMROOT%\SYSTEM32\DRIVERS\ETC` directory are created with DNS changes when saved. The HOSTS and HOSTS.PUB files correspond to DNS names for inside and outside hosts respectively. Outside DNS queries are done on the HOSTS.PUB file and inside DNS queries are done on the HOSTS and HOSTS.PUB files. The HOSTS and HOSTS.PUB files for the firewall setup are listed in Appendix A.

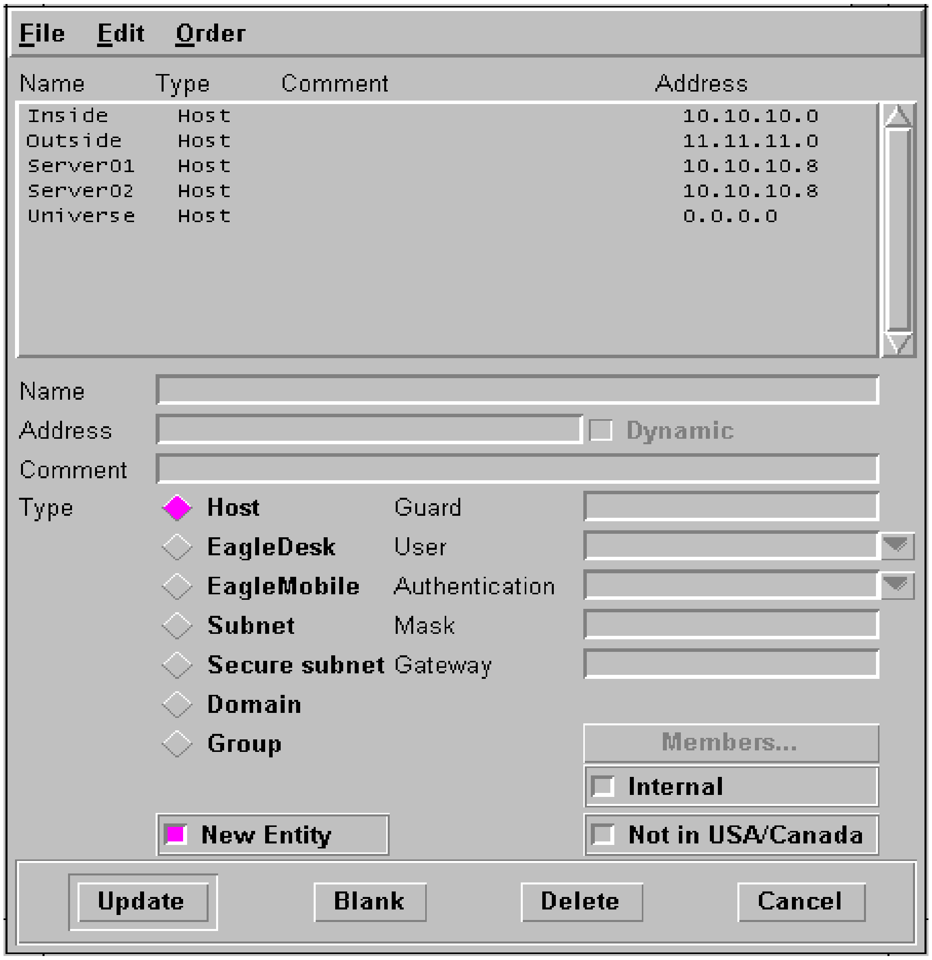
Since access is allowed from the DMZ/Hostile network to the private webserver for benchmark testing, configuration for the private webserver is done through the **`Gateway`** screen `File->Set up HTTP...` The physical server holds the address of `10.10.10.8` and is assigned the DNS names of server01 and server02 to create two virtual servers. Port 80 is used for both the inside port of the webserver daemon and the firewall gateway. Please refer to Screen 1, the **`HTTP Setup`** screen.



Proxy Host
Proxy Port #
Inside Host 10.10.10.8
Inside Port # 80
Gateway Port # 80
Extensions .gif .htm .html .jpg .txt .zip

Screen 1: **Http Setup**

Names given to network segments, hosts, groups, etc. are configured in the **`Net Entities`** screen. Rules can be applied based on names, once the network entities are configured. Inside, Outside, Server1, Server2, and universe are names for network entities needed in the firewall configuration. Please refer to Screen 2 for configured network entities.



Name	Type	Comment	Address
Inside	Host		10.10.10.0
Outside	Host		11.11.11.0
Server01	Host		10.10.10.8
Server02	Host		10.10.10.8
Universe	Host		0.0.0.0

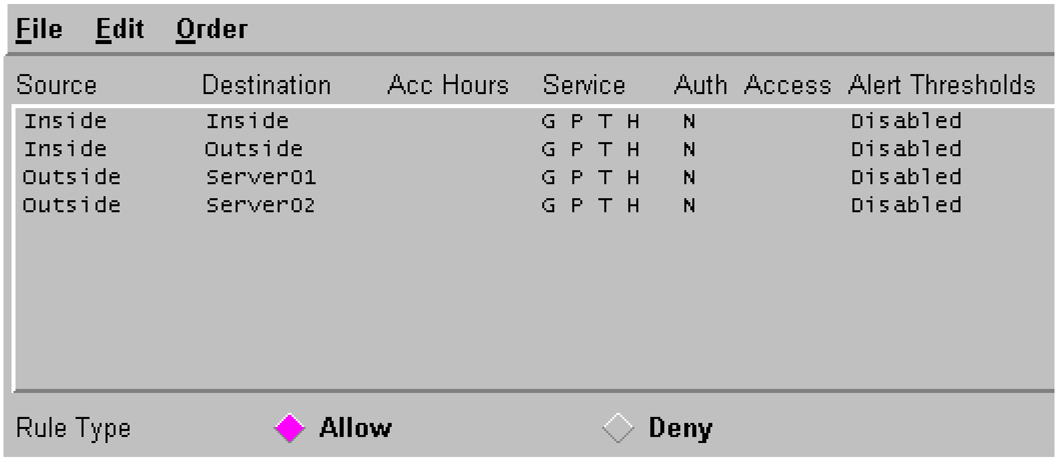
Name
Address □ Dynamic
Comment
Type ◆ Host ◇ EagleDesk ◇ EagleMobile ◇ Subnet ◇ Secure subnet ◇ Domain ◇ Group
Guard
User
Authentication
Mask
Gateway
□ Internal
■ New Entity
□ Not in USA/Canada

Screen 2: **Network Entries**

Eagle NT promotes transparency of IP addresses, meaning the only IP address the DMZ/Hostile zone can see is the outside interface of the firewall. Specifically, FTP transfers from the outside to the inside must first be connected to the firewalls outside interface, the FTP username becomes **Error! Reference source not found.**, and the password becomes the password for FTP at the FTP server. More authentication may be required by the firewall depending on the rule set. HTTP transfers from the outside to the inside must be directed to the firewalls outside interface. If an inside HTTP server has been configured as in Screen 2, the firewall checks the rule base to ensure that traffic is allowed to pass, then makes a connect request to the Web server. The client on the outside sees only the destination and source IP addresses of the outside interface of the firewall in the IP packet header. This technique is similar to address translation, except in an application firewall such as the Eagle NT 3.06, you get this feature for free.

Finally, the rules are configured to allow access from Private clients to Private servers, Private clients to DMZ/Hostile Servers, and DMZ/Hostile clients to specified Private servers. The convention of Inside and Outside mapping to Private and DMZ/Hostile was used. Also, note that specific rules must exist for access from the DMZ/Hostile network to the private network. Refer to the Screen 3, the **`Authorization`** screen.

FTP setup is also done at the **`Authorization`** screen. All rules have the FTP GET check box selected.



Source	Destination	Acc Hours	Service	Auth	Access	Alert Thresholds
Inside	Inside		G P T H	N		Disabled
Inside	Outside		G P T H	N		Disabled
Outside	Server01		G P T H	N		Disabled
Outside	Server02		G P T H	N		Disabled

Rule Type ◆ Allow ◇ Deny

Screen 3: **Authorization Rules**

Alert Thresholds track the number of times a particular client has connected through the firewall in a given time period. For the purposes of benchmark testing, this feature was disabled so that it would not skew transaction times.

HARDWARE AND SOFTWARE TUNING CHARACTERISTICS

In order to determine the affect in performance of the firewall system, software and hardware changes were evaluated and compared to a base system. Only one software/hardware configuration change at a time was made from the base system to determine the affect it may have. Since only one change is ever made to the base system for every benchmark run, decisions can be made to change firewall configurations in order to increase performance. It also allows those decisions to be made based on sets of individual configuration changes, since multiple individual changes can lead to higher performance than one individual change.

This section discusses hardware and software characteristics used in the benchmark tests. It also describes in detail, how to make the configuration changes in hardware and software so it can be referenced at a later time.

Hardware Characteristics

The various hardware options used in the tests are described below. Each hardware configuration change made was re-configured using the Compaq system partition utilities found by pressing the F10 key during the system bootup process.

Processor

Processor	MHz
Pentium Pro Uni and Dual,	200, 512KB cache
Pentium Pro	200, 256KB cache
Pentium	133
Pentium	120

RAM

RAM MB
32
64
128
256

Bus Subsystem

Bus Type - EISA and PCI
Compaq NetFlx-3 10/100 card
Compaq S2-Array Controller card

Drive Controller / Disks

Drive Controller	Disks
Compaq S2-Array Controller PCI	Raid 0 - No Fault Tolerant, 1 and 5 disks, Pagefile size = 200
Compaq S2-Array Controller EISA	Raid 0 - No Fault Tolerant, 1 disk. Pagefile size = 200
System ON BOARD SCSI Controller	1 disk. Pagefile size = 200

Network

Network
100 Mb
10 Mb

Software Characteristics

Eagle NT 3.06 switches, HTTP cache and DNS lookup

There are three switches used in the configuration of the Eagle NT 3.06 firewall that may increase performance on the HTTP daemon proxy. HTTP switches can be changed by editing the `%EAGLEDIR%\sg\startgw.cmd` file. They are:

- The `-f` switch controls the HTTPD performance speedup (via cache enabling/disabling). By default, using SmartStart, performance enhancement is enabled. Specify `-f 0` to disable it.

- The **`-y`** switch disables DNS lookups of source addresses when HTTP analyzes incoming connections. Default installations do not use this switch.
- The **`-z`** switch disables DNS lookups of destination addresses when HTTP analyzes incoming connections. Default installations do not use this switch.

In using these switches to gain performance on HTTP transfers, some restrictions do apply:

- Alert thresholds for all HTTP rules are disabled. This is not usually a problem. Since HTTP traffic is so bursty by nature, even the highest alert thresholds are often exceeded.
- HTTP connections do not appear in Hawk's Gateway window. This is not usually a problem since HTTP connections are so short-lived.
- HTTP connections that have exceeded a time limit or time range are not automatically killed.
- Messages in the Eagle log file do not display the number of the rule being used.

Number of rules used or rule base

The NSTL setup requires a minimum of 4 rules, which are used for most tests. Rule sets of 100 were also used to compare the performance difference in scanning the rule base.

Protocols used during test configurations

Tests are done using FTP and HTTP protocols and just the HTTP protocol. In both sets of tests a base system is used and the software and hardware difference is measured from the base system.

MaxReceive buffer changes on the NetFlx-3 NIC cards

Using the Windows NT Registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\cpqnf3(#)\Parameters

Add the following parameter:

MaxReceives = REG_DWORD 0x1F4 = 500

- Increases the number of MaxReceives counters for Compaq Netelligent 10/100TX Network Controller to 500. (The default is 100.)
- Specifies the maximum number of receive lists the driver allocates for receive frames

Base System

- ProLiant 5000 system
- 1-Pentium Pro 200 MHz Processor, 512K cache
- 64 MB RAM
- 2-EISA NetFlx-3 Network Interface Cards
- PCI Smart/2-Array controller, 1Disk, Raid 0
- MaxReceive Buffer for NetFlx-3 cards equals 100
- 100 Mb Network
- HTTP cache is ON
- DNS Lookups for HTTP is ON

TEST CONFIGURATIONS OF THE FIREWALL

The table below represents the different configurations using the Compaq ProLiant 5000 System. A * on the row indicates the configuration option that changed from the base system. The first test run is the base system.

Test Run	Processor Type and MHz	RAM MB	NIC BUS	Disk/Drive Controller, BUS	MaxRecv # Buffers	Network Mb	HTTP Cache/ DNS Lookup- HTTP/ Rules
1	PP200,512c	64	EISA	1/S2-A, PCI	100	100	on/on/4
2	PP200,512c	*128	EISA	1/S2-A, PCI	100	100	on/on/4
3	PP200,512c	*256	EISA	1/S2-A, PCI	100	100	on/on/4
4	PP200,512c	64	*PCI	1/S2-A, PCI	100	100	on/on 4
5	PP200,512c	64	EISA	1/S2-A, PCI	100	100	on/*off/4
6	PP200,512c	64	EISA	1/S2-A, PCI	100	100	*off/on/4
7	PP200,512c	64	*PCI	1/S2-A, PCI	100	*500	on/on/4
8	PP200,512c	64	EISA	1/S2-A, PCI	100	*500	on/on/4
9	*2 PP200,512c	64	EISA	1/S2-A, PCI	100	100	on/on/4
10	PP200,512c	64	EISA	1/S2-A, PCI	*10	100	on/on/4
11	*2 PP200,512c	*256	*PCI	1/S2-A, PCI	100	*500	on/*off/4
12	PP200,512c	64	EISA	*ON BOARD	100	100	on/on/4
13	PP200,512c	64	EISA	*1/S2-A, EISA	100	100	on/on/4
14	PP200,512c	64	EISA	1/S2-A,PCI	100	100	on/on/*100
15	PP200,512c	64	EISA	*5/S2-A, PCI	100	100	on/on/4

Runs 16, 17, 18 listed in the table below are for the Compaq ProSignia 500, ProLiant 800, and ProLiant 4500 respectively. These runs were done to show differences between hardware configurations and processor speeds.

Run	Processor Type and MHz	RAM MB	NIC BUS	Disk/Drive Controller, BUS	MaxRecv #Buffers	Network Mb	HTTP Cache/ DNS Lookup- HTTP/ Rules
16	P120	32	EISA	ON BOARD	500	100	on/off/4
17	PP200,256c	32	PCI	ON BOARD	500	100	on/off/4
18	P133	128	EISA	ON BOARD	500	100	on/off/4

The test runs labeled below correspond to HTTP only tests. These tests are done on the ProLiant 5000. Test 19 is considered as a base system for HTTP only traffic through the firewall. Again the * represents the change from the base system.

Run	Processor Type and MHz	RAM MB	NIC BUS	Disk/Drive Controller, BUS	MaxRecv #Buffers	Network Mb	HTTP Cache/ DNS Lookup-HTTP/ Rules
19	PP200,512c	64	EISA	ON BOARD	100	100	on/on/4
20	PP200,512c	64	EISA	ON BOARD	100	100	on/*off/4
21	PP200,512c	64	EISA	ON BOARD	100	100	*off/on/4
22	PP200,512c	64	EISA	ON BOARD	100	100	on/on/*100

EVALUATION OF RESULTS

The results of these benchmark tests are categorized by hardware and software differences from the base system. The results are calculated in transactions per minute for each run. Failures are examined as they provide insight to particular gains or losses. Exactly one hardware or software configuration change is made to the base system for each run. Sets of test runs are completed using different hardware and software configurations each providing a change to the base system. These runs are compared to the base system to determine percent differences between the test runs. Percent differences from transactions per minute differences are then evaluated on a positive and negative basis to show more clearly the affects the particular hardware or software configuration change made to the system. Understanding these positive and negative differences from the base system run explains individual hardware or software performance gains or loses in the system. Sets of individual performance gains or losses can then be assessed to determine what can be done to improve total performance of the firewall.

A high-end system was used as the base line for test runs evaluated in this paper, which allowed tests to be run more quickly. Theoretically, the same performance gains or positive percent differences from hardware and software configuration changes used in the high-end system can be achieved using a low-end system as well, providing the firewall software does not change. This allows decisions to be made to increase performance on lower-end systems where it makes sense to have a lower end firewall system such as in small companies, branch offices, or schools.

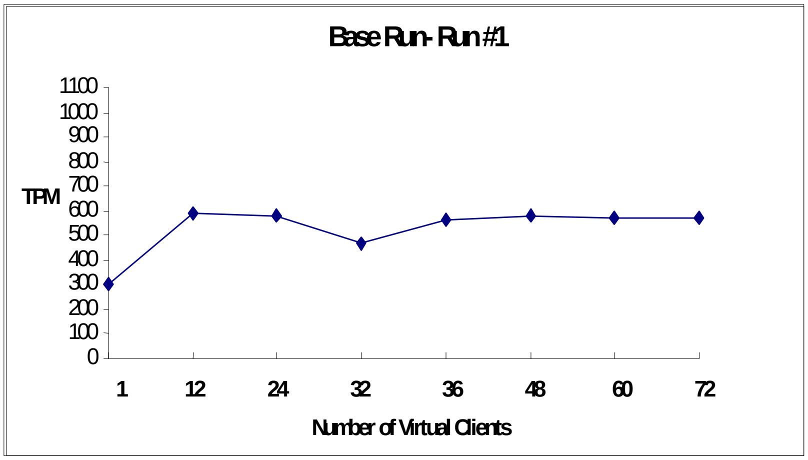
The goals of this section are to provide and explain the results of the test runs and to help the reader gain an understanding of what can be done to improve the performance of the firewall system. This section is broken down into two parts based on test runs with HTTP and FTP transactions and test runs with HTTP only transactions. In both parts, results of the base run are described first, and then the other runs are described and compared to the base run. The results to all of the tests can be found in Appendix B.

Tests results with HTTP and FTP Transactions

This section first describes the base system results then displays the results and describes the effect that each hardware and software characteristic has on the base system. The ordering of subsections are based on test runs listed in Table 1 and Table 2 of Test Configurations of the Firewall section. Subsections are Base System, Memory, NIC Bus Type, DNS Lookups for HTTPD, HTTPD Cache, MaxRecieve Buffers for NetFlx-3 Cards, Processor, Network Speed, Disk Controller, 100 Firewall Rules, Full System, Other Systems and Configurations. The last subsection contains some test runs based on lower end ProLiant and ProSignia systems and was run to show performance on lower-end systems.

Base System

The base system, test run 1, consists of the ProLiant 5000 system, 1Pentium Pro 200 MHz, 512K cache processor, 64 MB RAM, 2-EISA NetFlx-3 10/100, PCI Smart/2-Array Controller Raid 0, 1 SCSI Disk, MaxReceive Buffers is 100, HTTPD cache is on, DNS Lookups for HTTPD is on, and 100Mb Network. The graph of the base system run is displayed in Graph 1.

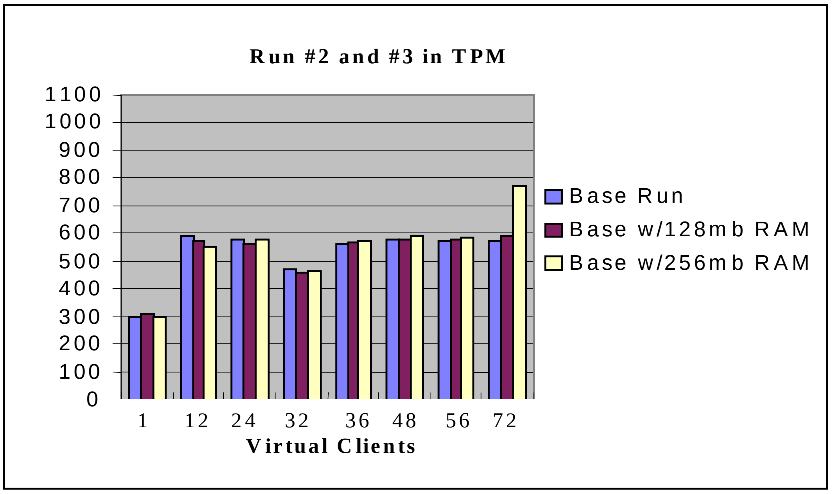


Graph 1: **Base Run for HTTP and FTP Transactions**

The jump from 300-TPM on 1 virtual client to 590-TPM on 12 virtual clients is expected as the load increases on the system. The slight dip to 470-TPM on 32 virtual clients is due to garbage collection and cleanup of the firewall system and is noticed throughout all of the test runs. From 36 virtual clients through 72 virtual clients the TPM is maintained steadily between 560-TPM's through the 570-TPM's. The average number of failures for all runs was under 1%.

Memory

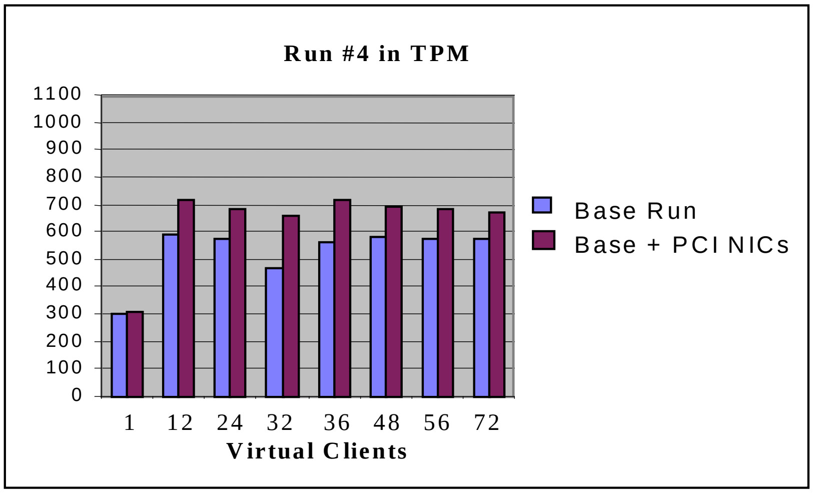
Run #2 and #3 increase memory from the base system up to 128 MB and 256 MB respectively. Raptor's Eagle NT 3.06 product is made to run with no less than 32 MB with a static virtual memory size of 200 MB. As displayed in Graph 2, increasing the memory of the firewall system only adds performance value when the load gets heavier. Tests with 36 to 72 virtual clients show increases in performance up to 3%, where 12 to 32 virtual clients show decreases in performance by 1-2% for lighter loads, for both memory scenarios. The reason for this behavior is that the firewall only needs a set amount of memory to process connections. Once the connection is established for each virtual client, the process of moving data between the incoming connection and outgoing connection does not require the use of more memory.



Graph 2: **Base Run with 128 MB and 256 MB RAM**

NIC Bus Type

Two PCI NetFlx-3 10/100 NICS replaces two EISA Netflx-3 10/100 for this test. The graph of this run is displayed in Graph 3.



Graph 3: **Base Run with PCI NICs**

The percent difference increase in TPM from the base reached 29% at 32 virtual clients then leveled to around 16% increase from the base system at 72 virtual clients. The burst in TPM at 32 virtual clients to 36 virtual clients comes from garbage cleanup of the firewall system. Improvements are caused from the PCI bus speed being faster than the EISA bus. The average failure rate for all runs is under 1%.

DNS Lookups for HTTPD, HTTPD Cache

DNS lookups turned off for Run #5 results in an average overall percent increase from the base system in TPM of 4%. Peaks from the base system of 16% to 31% TPM increases are attributed to time just after system cleanup procedures. Since HTTP and FTP are tested in this run there is not a big increase in performance since FTP transfers are still doing DNS Lookups. On HTTP only transfers, the TPM and the percent TPM difference increase from the base system is higher because the HTTP daemon supports the switch for no DNS Lookups and FTP currently does not. Please refer to section Test Results with HTTP Only for HTTP only test results.

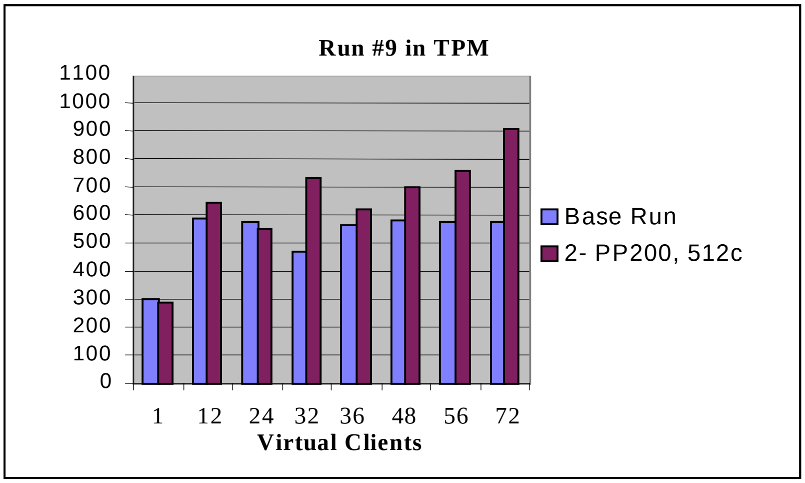
Turning off HTTP caching of the rules, run #6, degrades performance overall by 1% from the base system with a peak low of 4%. The overall average failure rate for both tests is less than 1% from the base system. The performance degradation is expected since caching allows the rule base only to be checked once a minute as opposed to every connection. Allowing HTTP caching of the rules especially improves performance if the rule base is large.

MaxRecieve Buffers for NetFlx-3 Cards

Setting the MaxRecieve buffers for the NetFlx-3 NIC cards to 500 represented by Run #7 and Run #8. Run #7includes the MaxRecieve Buffers change and 2 PCI Netflx-3 cards. This results in an overall 16% increase from the base system. Run #8 displayed negative differences of 5% from the base system for 1 to 24 virtual clients and increased as the load increased to an average of 5.6% above the base for 32 to 72 virtual clients. The overall average for all percent differences for 1 to 72 virtual clients was 1.6%. Failures decreased from the base system to overall 0.02% for all virtual client runs.

Processor

In Run #9, a Pentium Pro 200 MHZ-512 cache processor was added to the base system. Review Graph 4 below for results.



Graph 4: **Base Run with 2 Processors**

Adding the second processor clearly shows performance improvements to the TPM from the base system. The overall average percent difference increase from the base system for all virtual clients is 15%. As the load increased, the TPM is increased bringing the positive percent difference to over 36% from the base system with 72 virtual clients. Failures increased slightly to 2% overall for all virtual clients. The increase in TPM is due to the use of IO Completion ports and threads in the HTTPD of Raptors Eagle NT 3.06 firewall software.

Network Speed

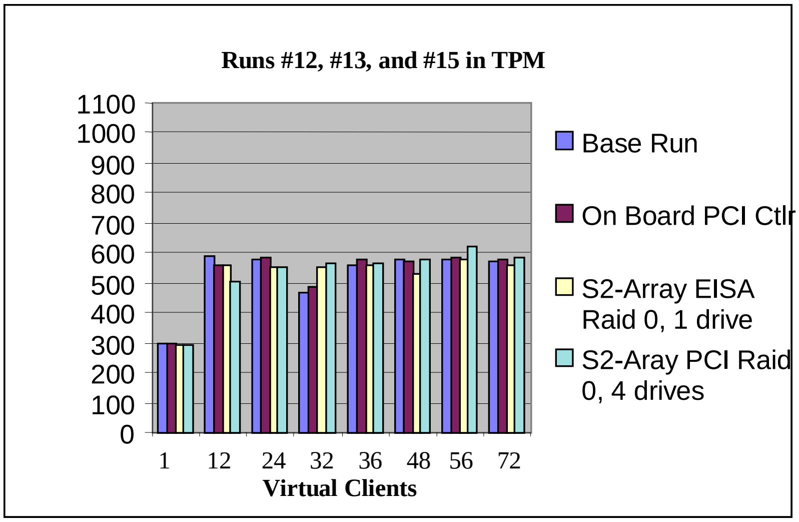
In Run #10, the 100Mb hubs were replaced with 10Mb hubs to show the degradation of performance by the network. The overall negative percent difference that was shown by the network, from 1 to 72 virtual clients, was 2%. The lows were down to 10% negative difference for 24 virtual clients and 7% negative percent difference for 48 virtual clients from the base system. The purpose was to show how the network affects performance. Theoretically, the collision rate on the 10Mb network would be higher under such loads than the 100Mb network and thus the performance degrade. To show that the firewall can handle throughputs of more than 10Mb per second please refer to the Other Systems and Configurations subsection and Test Results with HTTP Only section.

100 Firewall Rules

Run #14 applied 100 rules to the firewall rule set to show the performance hit on the firewall system. The overall performance decrease by using 100 rules, was 16% from the base system. These rules included adding user-defined protocol as well as most of the standard protocols found in the SERVICES file. The reasons for the decline is that the FTP daemon does not support caching of the rules so each packet is checked via the rule base as it is routed through the firewall. HTTP, however, does support caching of the rules. The HTTPD cache is updated by the rule base once per minute. HTTP only transfers provide less of a performance hit on the firewall system as described in the section Test Results with HTTP Only.

Disk Controller

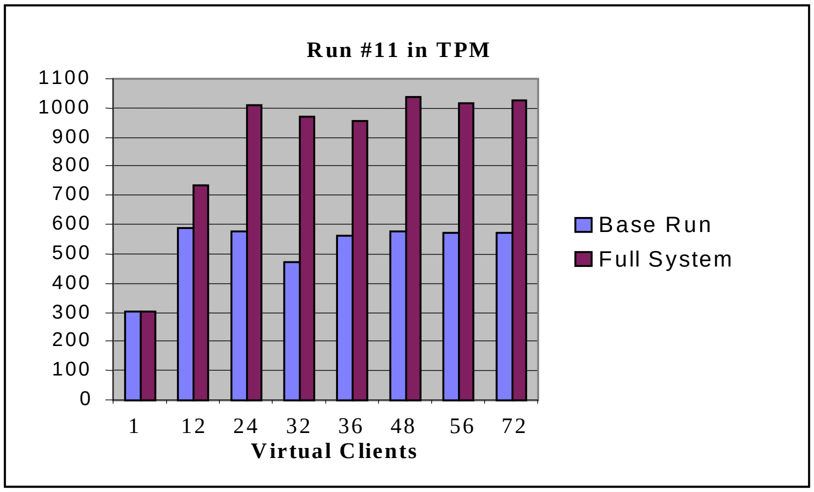
The base run used a PCI Smart-2 Array Controller card with 1 disk at Raid 0. The tests here show the ON BOARD PCI SCSI Controller, EISA Smart-2 Array Controller card with 1 disk at Raid 0, and Smart-2 Array Controller PCI with 4 disks at Raid 0. Raid 0 possesses the highest performance to disk IO but provides no mechanism for data recovery. These tests were run to show what affect the disk controller/disk combination used with Raid 0 had on the writes to the log file from the firewall software. Logging was moderate to heavy, tracking every connection, disconnect, FTP GET, rules authorization for HTTP and FTP, and other FTP statistics. Each log file contained 8 to 10 megabytes of data after each run. The overall average percent differences for runs #12, #13, and #15 did not exceed 0.05%. This small performance difference is attributed to the fact that Raptor's Eagle NT 3.06 Firewall system flushes log file information in batch processes. For heavy loads, log file writes are done every few seconds instead of updating the log file for every system event. This allows the firewall to concentrate more on passing data than writing log file information and stops the log file generator from being a bottleneck on the system.



Graph 5: **Base Run with On Board PCI Ctlr, S2-Array EISA-R0-1D, S2-Array PCI-R0-4D**

Full System

Run #11 adds a Pentium Pro 200-512K cache processor, 256 MB RAM, sets MaxRecieve buffers for NetFlx-3 cards to 500, changes to PCI bus for NIC cards, and sets DNS Lookups for HTTPD off. Adding these features together shows, the combined performance enhancements. Refer to Graph 6 for the results.



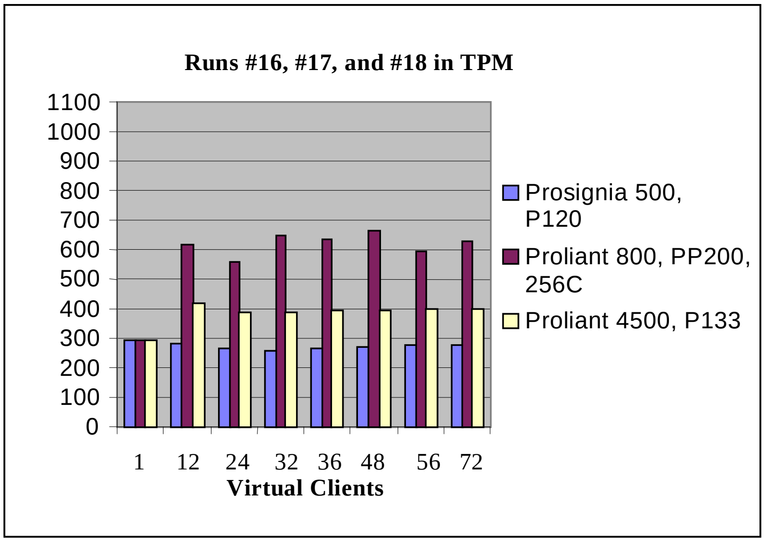
Graph 6: **Full System**

The overall average percentage increase from 1 to 72 virtual clients is 36%. As the load gets higher from 24 to 72 virtual clients the average percentage increase is 44% with peaks of 52% for 32 virtual clients. Failures are less than 0.5%.

Other Systems and Configurations

This section includes test runs with other systems and configurations. It also includes other runs using the base system described above with other configurations.

Graph 7 includes runs #16, #17, and #18 for ProSignia 500, ProLiant 800, and the ProLiant 4500 respectively. These runs should not be compared to the base system because of the configuration and hardware differences. Descriptions of these three machines and their configurations are listed in the section Test Configurations of the Firewall.



Graph 7: **ProSignia 500, ProLiant 800, ProLiant 4500**

The low-end server, the ProSignia 500, had an overall average of 273 TPM for all virtual clients pushing almost an estimated 1.9Mb per seconds through the system. The ProLiant 800 had an overall average for all virtual clients of 620 TPM with a high of 665 TPM at 48 virtual clients. The ProLiant 4500 had an overall average of 398 TPM for its virtual client runs. The average failure rates for these test runs are less than 1%.

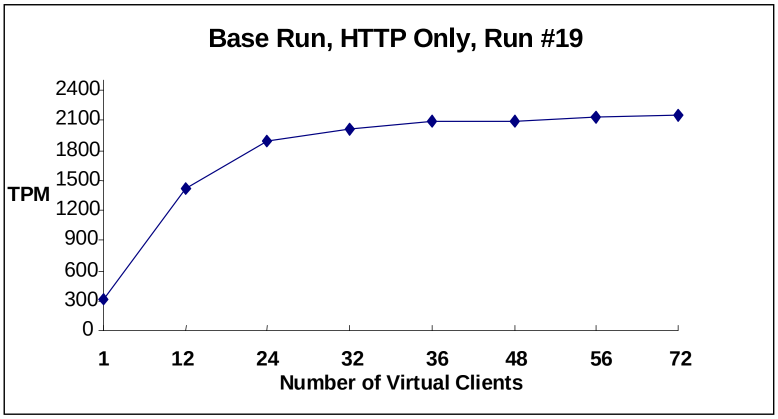
Another test run on the base system showed that the firewall could handle more than 10Mb of traffic through the firewall for HTTP and FTP transfers. This test added the number of virtual clients to a total of 144 virtual clients on 8 physical client machines. The test results show that the TPM was 1696 and 10.67Mb throughput was calculated for data passing through the firewall.

Tests Results with HTTP Only

The same model is used for HTTP only sets of tests as for the tests with HTTP and FTP. The same base system is used with no changes except that 100 percent of the traffic is HTTP traffic. The benchmark is run using the base system with the same test bed setup, 3 physical servers and 8 physical clients, with 1 to 72 virtual clients and 6 virtual servers. The set of tests run in this section were designed to show the performance increases that had been made to the HTTP daemon. These increases in performance from the HTTP daemon are attributed to the threaded enhancement, the use of IO completion ports, and caching of the rules. This section presents the Base Run, DNS Lookups for HTTPD and HTTP Cache, and 100 Rules.

Base Run

The base system, test run 1, consists of the ProLiant 5000 system, 1Pentium Pro 200 MHz, 512 cache processor, 64Mb RAM, 2-EISA NetFlx-3 10/100, PCI S2-Array Controller Raid 0, 1 SCSI Disk, MaxReceive Buffers is 100, HTTPD cache is on, DNS Lookups for HTTPD is on, and 100Mb Network. The graph of the base system run is displayed in Graph 8.

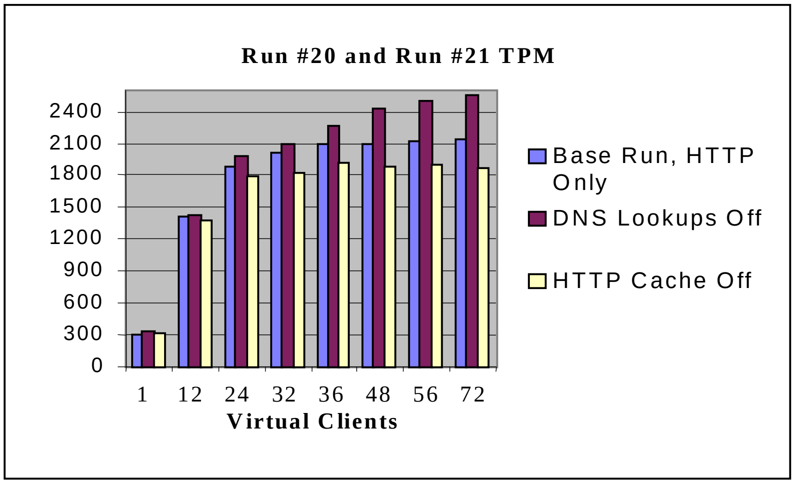


Graph 8: **Base Run, HTTP Only**

As you may notice HTTP only Transactions Per Minute are three times the TPM as seen with HTTP and FTP transactions. The overall TPM for 2 to 72 virtual clients 2 was 1966. As the load increases the TPM increases to a high 2146 TPM at 72 virtual clients. The failure rate was 0.0%. The calculated highest throughput is 15Mb for 72 virtual clients.

DNS Lookups for HTTPD and HTTP Cache

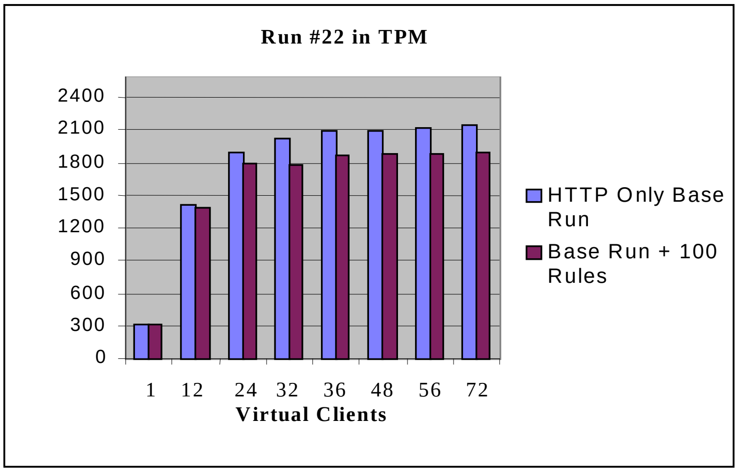
Run #20 turns the DNS Lookup for HTTP switch off and Run #21 turns off the HTTP Cache switch. Refer to Graph 9 for the results. DNS Lookups off yields in a 9% increase from the base where not caching rules for HTTP results in 7% degradation from the base system. Failures remained at 0.0%.



Graph 9: **Base Run, DNS Lookups Off, HTTP Cache Off**

100 Rules

Run #22 applies 100 rules to the firewall rule set to show the decrease in performance. Graph 10 displays the decrease in performance.



Graph 10: **Base Run and 100 Rules**

The overall average percent decrease in performance from the base system for virtual clients 1 to 72 was 7%. The trend tends to decrease in performance as the number of virtual client's increases and leveling off at about 11.5% performance decrease from the base at 72 virtual clients. The percent failure is 0.0% for all sets of virtual clients. This decrease in performance with a rule set of 100 rules is expected because of the extra time needed to ensure that all packets passed through the firewall system meet the security requirements of the rule set.

CONCLUSIONS

For hardware configurable tests, upgrading the Network Interface Cards from the EISA bus to the PCI bus resulted in noticeable increases in performance. The processor scales well when moving from one processor to two processors, making appreciable increases in performance and increased performance as the load increases. Increasing memory adds slight performance increases. The drive controller tests from EISA Smart-2 Array Controller Raid 0, PCI Smart-2 Array Controller Raid 0 and Raid 5, and ON BOARD PCI Controller gave expected results and minimal performance increases because of performance enhancements made to the firewall to allow log file writes to be done in batch processes instead of writing log file information for every event. Network speed also gave expected results when going from a 100Mb network to 10Mb network. The firewall was able handle throughput of more than 10Mb for both HTTP/FTP and HTTP only transfers.

Software configurable tests with HTTP Cache on drew expected increases in performance in both HTTP/FTP and HTTP only tests. This software switch is turned on by default in SmartStart installations of Raptor’s Eagle NT 3.06 product to give higher performance using the cache from the time of installation. No DNS Lookups for HTTP displayed slight performance increases for FTP/HTTP transfers but presented high performance increases for greater loads on HTTP Only tests. Expected decreases were noticed in both HTTP/FTP and HTTP only test runs when not using HTTP caching of rules.

Differences between HTTP/FTP and HTTP only transfers displayed enormous performance increases for HTTP only transfers showing the added performance enhancements included in Raptor’s Eagle NT 3.06 firewall product.

This paper gives information about performance enhancements for firewalls using various hardware and software components also take into account the protection and security gained by using a firewall and should notice that there is a performance hit in using a firewall for any environment. As a result, using Compaq servers and adding specific hardware and software components can reduce this performance hit dramatically while increasing overall performance of the firewall for your environment.

APPENDIX A

DNS `hosts` and `host.pub` files for Raptors Eagle NT 3.06 firewall setup.

%systemroot%\system32\drivers\etc\hosts

```
10.10.10.50     aaa.testbed.com   aaa

10.10.10.1      client01.testbed.com    client01
10.10.10.2      client02.testbed.com    client02
10.10.10.5      client03.testbed.com    client03
10.10.10.4      client04.testbed.com    client04
10.10.10.6      client05.testbed.com    client05

10.10.10.8      server01.testbed.com    server01
10.10.10.8      server02.testbed.com    server02

10.10.10.50     firewall01.testbed.com  firewall01

127.0.0.1         localhost
# forward_to
# authority testbed.com
# authority 127.in-addr.arpa 10.10.10.in-addr.arpa
# inside_interface 127.0.0.1
# inside_interface 10.10.10.50
```

%systemroot%\system32\drivers\etc\hosts.pub

```
11.11.11.50     aaa.testbed.com         aaa

11.11.11.2      client06.testbed.com    client06
11.11.11.3      client07.testbed.com    client07
11.11.11.4      client08.testbed.com    client08

11.11.11.7      server03.testbed.com    server03
11.11.11.7      server04.testbed.com    server04
11.11.11.8      server05.testbed.com    server05
11.11.11.8      server06.testbed.com    server06

11.11.11.9      client01.testbed.com    client01

11.11.11.50     firewall02.testbed.com  firewall02
11.11.11.50     firewall03.testbed.com  firewall03
# authority testbed.com
# authority 127.in-addr.arpa 11.11.11.in-addr.arpa
```

APPENDIX B

Run1	Users	URLS	TPM	%Failures
	1	100	300.26	0.00
	12	1200	589.78	0.67
	24	2400	577.98	0.54
	32	3200	469.58	1.44
	36	3600	560.95	0.78
	48	4800	579.20	0.75
	60	6000	574.46	0.90
	72	7200	573.71	0.75
Run2				
	1	100	311.12	0.00
	12	1200	573.55	0.25
	24	2400	561.20	0.63
	32	3200	456.49	1.50
	36	3600	566.68	0.72
	48	4800	576.39	0.83
	60	6000	580.88	0.80
	72	7200	592.19	7.56
Run3				
	1	100	296.19	0.00
	12	1200	549.55	0.92
	24	2400	576.93	0.92
	32	3200	462.17	1.41
	36	3600	572.76	1.06
	48	4800	588.60	6.48
	60	6000	583.49	0.75
	72	7200	771.93	13.89
Run4				
	1	100	305.70	0.00
	12	1200	716.57	0.67
	24	2400	681.76	0.75
	32	3200	661.02	1.09
	36	3600	718.58	0.81
	48	4800	691.96	0.81
	60	6000	683.09	0.68
	72	7200	674.38	0.92
Run5				
	1	100	292.30	0.00
	12	1200	506.52	1.08
	24	2400	564.22	0.92
	32	3200	560.42	0.88
	36	3600	582.75	0.78
	48	4800	568.30	0.92
	60	6000	579.57	0.90
	72	7200	835.37	16.00
Run6				
	1	100	306.33	0.00
	12	1200	565.48	0.17
	24	2400	554.12	0.83
	32	3200	552.09	0.94
	36	3600	559.47	0.94
	48	4800	561.13	0.77
	60	6000	566.58	0.75
	72	7200	600.01	10.65
Run7				
	1	100	308.24	0.00
	12	1200	714.64	0.50
	24	2400	673.06	0.96
	32	3200	659.95	1.03
	36	3600	695.06	0.97
	48	4800	677.40	0.73
	60	6000	678.28	1.00
	72	7200	688.15	0.81
Run8				
	1	100	285.90	0.00
	12	1200	532.56	1.00
	24	2400	575.57	0.71
	32	3200	591.38	0.66
	36	3600	576.93	0.81
	48	4800	573.12	1.00
	60	6000	598.64	0.72
	72	7200	584.61	0.71

```
Run9     Users    URLS     TPM      %Failures
         1        100      288.80   0.00
         12       1200     641.81   0.92
         24       2400     550.35   1.42
         32       3200     732.57   1.44
         36       3600     616.26   1.47
         48       4800     701.10   4.60
         60       6000     753.75   1.45
         72       7200     906.89   11.79
Run10
         1        100      267.27   0.00
         12       1200     580.00   0.00
         24       2400     520.36   1.38
         32       3200     537.21   1.03
         36       3600     551.82   1.03
         48       4800     536.85   0.88
         60       6000     616.07   10.42
         72       7200     547.19   0.79
Run11
         1        100      303.77   0.00
         12       1200     732.67   0.92
         24       2400     1008.81  1.13
         32       3200     969.93   1.50
         36       3600     953.11   1.39
         48       4800     1035.70  1.38
         60       6000     1017.86  1.45
         72       7200     1025.60  1.42
Run12
         1        100      299.24   0.00
         12       1200     557.59   0.83
         24       2400     586.42   0.83
         32       3200     487.19   1.44
         36       3600     580.02   0.75
         48       4800     568.59   0.77
         60       6000     582.80   0.70
         72       7200     576.25   0.63
Run13
         1        100      294.33   0.00
         12       1200     557.22   1.00
         24       2400     556.05   0.63
         32       3200     551.05   0.63
         36       3600     562.02   0.58
         48       4800     529.13   5.98
         60       6000     574.37   0.77
         72       7200     558.48   0.75
Run14
         1        100      306.03   0.00
         12       1200     464.38   17.25
         24       2400     415.19   23.08
         32       3200     416.76   23.63
         36       3600     424.62   26.69
         48       4800     425.15   25.04
         60       6000     433.59   25.95
         72       7200     583.23   30.29
Run15
         1        100      292.96   0.00
         12       1200     503.57   1.08
         24       2400     552.47   0.71
         32       3200     565.54   1.00
         36       3600     566.47   0.72
         48       4800     575.06   0.69
         60       6000     617.53   6.90
         72       7200     584.06   0.56
Run16
         1        100      295.84   0.00
         12       1200     281.50   0.00
         24       2400     261.88   0.00
         32       3200     260.43   0.00
         36       3600     265.96   0.00
         48       4800     270.98   0.00
         60       6000     275.88   0.00
         72       7200     273.82   0.00
```

```
Run17   Users   URLS    TPM     %Failures
        1       100     291.91  0.00
        12      1200    618.30  0.33
        24      2400    558.30  1.38
        32      3200    646.74  1.00
        36      3600    634.72  1.00
        48      4800    665.94  0.77
        60      6000    595.91  1.03
        72      7200    626.93  0.78
Run18
        1       100     291.91  0.00
        12      1200    417.71  0.08
        24      2400    389.75  0.50
        32      3200    390.26  0.41
        36      3600    395.33  0.28
        48      4800    394.27  0.27
        60      6000    402.16  0.23
        72      7200    400.86  0.18
Run19
        1       100     307.40  0.00
        12      1200    1408.41 0.00
        24      2400    1889.15 0.00
        32      3200    2016.70 0.00
        36      3600    2085.60 0.00
        48      4800    2092.46 0.00
        60      6000    2124.07 0.00
        72      7200    2145.73 0.00
Run20
        1       100     327.70  0.00
        12      1200    1433.30 0.00
        24      2400    1975.51 0.00
        32      3200    2098.05 0.00
        36      3600    2268.31 0.00
        48      4800    2428.20 0.00
        60      6000    2497.29 0.00
        72      7200    2557.15 0.00
Run21
        1       100     324.31  0.00
        12      1200    1377.35 0.00
        24      2400    1793.25 0.00
        32      3200    1830.79 0.00
        36      3600    1926.18 0.00
        48      4800    1881.94 0.00
        60      6000    1901.62 0.00
        72      7200    1867.28 0.00
Run22
        1       100     315.48  0.00
        12      1200    1385.41 0.00
        24      2400    1795.83 0.00
        32      3200    1785.91 0.00
        36      3600    1862.68 0.00
        48      4800    1878.33 0.00
        60      6000    1882.94 0.02
        72      7200    1897.30 0.00
```