WHITEPAPER

July 1997

Prepared By
Internet Solutions
Business Unit

Compaq Computer
Corporation

Performance Improvements of Raptor’s EagleNT 4.0 Firewall on Compaq Servers

This paper continues documenting Compaq’s performance testing of the Raptor EagleNT firewall by looking at Raptor’s latest release, version, 4.0. Please refer to the first firewall performance paper, ***Performance Analysis and Tuning of Raptor's Eagle NT 3.06 Firewall on Compaq Servers****, for information regarding the methodology used for firewall testing, as well as the performance test results for EagleNT 3.06.*

CONTENTS

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 NetFlex, registered United States Patent and Trademark Office.

Eagle, EagleNT 3.06, EagleNT 4.0, and Raptor are trademarks and/or registered trademarks of Raptor Systems Inc.

Microsoft, Windows, Windows NT are trademarks and/or registered trademarks of Microsoft Corporation.

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

"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 client's product. NSTL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO RESULTS TO BE OBTAINED BY ANY PERSON OR ENTITY FROM USE OF THE SERVICES OR THE RESULTS THEREOF, OR ANY INFORMATION OR DATA INCLUDED THEREIN. NSTL MAKES NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT TO THE SERVICES AND/OR RESULTS THEREOF, OR ANY INFORMATION OR DATA INCLUDED THEREIN."

Performance Improvements of Raptor's EagleNT 4.0 Firewall on Compaq Servers
First Edition (July 1997)
247A/0897ECG

INTRODUCTION

This paper describes the performance increases in Raptor's EagleNT 4.0 firewall over the previous version, EagleNT 3.06. By showing performance gains and losses associated with various hardware and software configurations, the paper allows logical decisions for performance increases in the firewall to be made.

The results reported here were achieved using the same test methodology as that established for version 3.06 [1]. This allows direct comparisons to be made between each version of the firewall. Performance increases of the new version over the previous version are attributable to support for Microsoft Windows NT 4.0 (EagleNT 3.06 supported Microsoft Windows NT 3.51) and to Raptor's engineering improvements for this version.

Among the new features of EagleNT 4.0 is WebNot, a filtering mechanism for objectionable material. The performance of this feature was also examined.

EXECUTIVE SUMMARY

This paper used the National Software Testing Labs (NSTL) software benchmark methodology to test the performance of the EagleNT 4.0 firewall. Various hardware and software configurations were tested including the following: Increasing memory, adding additional processors, changing the NIC bus, decreasing network speed, creating large numbers of firewall rules, blocking large numbers of objectionable URLs, and turning off Raptor's HTTP Cache and DNS Reverse Lookups. The results obtained from these configurations yielded the following conclusions:

- ❑ Overall performance of the EagleNT 4.0 firewall has increased in the following areas:
  - Transactions per minute (TPM) are up 90% on average.
  - Transaction failures (*connection related, **not failures of the firewall software***) have decreased.
  - Throughput has reached 22 megabits/sec.
- ❑ The number of firewall rules has no impact on performance.
- ❑ The WebNot URL-blocker does not affect performance.
- ❑ Changing network interfaces from EISA to PCI increases performance up to 30%.
- ❑ EagleNT 4.0 will process more data than can be transmitted over a 10 megabit/sec internal network. It can handle the data transmitted with approximately 14 T1 (1.54 megabits/sec) lines.
- ❑ The EagleNT 3.06 performance switches on the HTTP cache are no longer supported; however, DNS Reverse Lookups may now be shut off for all daemons with no performance impact.
- ❑ Increasing memory had no measurable effect on performance.
- ❑ Adding a processor(s) will affect performance, but only after significant throughput is attained. Significant throughput was achieved when PCI NICs were installed.
- ❑ Modifying Compaq's MaxReceives buffer for NetFlex-3 cards does not increase performance of the Raptor firewall.

[1] See Appendix A. Also, see Performance Analysis and Tuning of Raptor's Eagle NT 3.06 Firewall on Compaq Servers. (http://www.compaq.com/support/techpubs/whitepapers/278a0497.html).

NSTL TEST SUITE

The Raptor EagleNT 4.0 tests were run using the benchmark software from NSTL (Version 1.0). This benchmark uses a total of twelve machines: eight clients, three servers, and the firewall. Configuration files are used to specify the number of clients and servers running for each test, and the data that passes between them. Specific details about the NSTL configuration are available in the Appendix.

The NSTL benchmark reports performance in transactions per minute (TPM) and failures. The ***transaction*** in TPM includes opening a connection from the client to the server, requesting and downloading the data from the server, and closing the connection. A failure is any failure occurring during a transaction (that is, connection time-outs and dropped packets); **it is not a failure in the Raptor firewall software**. TPM and failures vary from run to run for the same configuration as demonstrated by the ten base system runs documented in Table 1. These variations will be addressed in the latest NSTL software (Version 2.0) by enforcing use of Service Pack 3 for Windows NT Server. The service pack contains fixes to the Microsoft implementaion of TCP/IP.

	1	2	3	4	5	6	7	8	9	10				
Clients	Transactions Per Minute (TPM)										stdev	avg	stdev %	2 stdev %
1	295.90	291.07	289.07	293.51	290.02	298.55	301.49	287.82	296.73	301.55	5.04	294.57	1.71	3.42
12	706.08	642.93	572.69	649.01	622.28	713.75	695.14	630.74	740.15	691.75	51.18	666.45	7.68	15.36
24	1323.35	1291.15	1319.40	1295.92	1311.39	1020.44	1298.17	1298.66	1314.31	1312.85	91.34	1278.56	7.14	14.29
32	1216.10	1237.23	1140.50	1127.85	1138.05	1247.59	1189.18	1127.37	1200.33	1147.93	46.44	1177.21	3.94	7.89
36	1146.69	1032.32	1117.75	1158.78	1123.52	1124.88	1131.02	1084.17	1159.27	1113.63	37.90	1119.20	3.39	6.77
48	1181.61	1137.15	1119.46	1150.37	1156.30	1128.59	1207.48	1130.67	1165.04	1148.27	26.75	1152.50	2.32	4.64
60	1260.70	1242.57	1226.92	1248.55	1204.72	1256.80	1219.15	1248.64	1257.87	1215.42	20.01	1238.13	1.62	3.23
72	1283.69	1352.10	1330.69	1296.29	1317.56	1307.96	1286.52	1326.94	1208.05	1252.07	41.93	1296.19	3.23	6.47
														7.76
	Failures %										stdev	avg	stdev %	2 stdev %
1	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
12	0.58	0.67	0.92	0.83	0.58	0.58	0.58	0.83	0.58	0.58	0.13	0.68	0.20	0.39
24	0.00	0.00	0.00	0.00	0.00	0.79	0.00	0.00	0.00	0.00	0.25	0.08	3.16	6.32
32	0.28	0.34	0.50	0.50	0.50	0.25	0.41	0.47	0.25	0.50	0.11	0.40	0.27	0.55
36	0.81	1.44	0.89	0.67	0.78	0.97	1.00	1.08	0.64	0.94	0.23	0.92	0.25	0.51
48	1.69	1.88	1.65	1.44	2.04	1.58	1.69	1.54	1.81	1.60	0.18	1.69	0.10	0.21
60	1.77	2.18	1.82	2.00	2.18	1.80	1.80	1.63	2.27	1.82	0.22	1.93	0.11	0.22
72	2.57	2.04	2.19	2.00	2.21	2.13	2.31	1.81	2.36	2.18	0.21	2.18	0.10	0.19
														1.05

Table 1. *The statistical analysis of ten base runs.*

To avoid attributing performance differences to a change in configuration when in fact the differences were due to the variability of the NSTL suite, a rudimentary statistical analysis was done on the data. First, the average and the standard deviation were calculated for the client load of each run. The standard deviation was then expressed as a percent. If a normal distribution is assumed, 68% of the data should be in a range one standard deviation away from the average, and 95% of the data should be within two standard deviations of the average. Thus, the last column of the table shows the standard deviation doubled. A simple average of the doubled standard deviation is taken, allowing one measure to be applied for any client load.

After this analysis, 95% of all data should yield a percent change of no greater than 7.76 in TPM, and no greater than 1.05 percent change in failures. In the testing of a configuration and subsequent comparisons to the base system, percent changes within these ranges were considered insignificant. Conversely, percent changes outside this range were attributed to the configuration being tested.

INDIVIDUAL RESULTS

The test methodology for EagleNT 4.0, including the test bed, the base system, and the testing software, was identical to that used for EagleNT 3.06 [2]. The configurations tested were also identical to those tested for EagleNT 3.06; however, configurations were added to test new features of the Raptor software while other configurations, which proved under EagleNT 3.06 to have no effect on performance, were eliminated. Table 2 summarizes the configurations tested with significant changes from the base system highlighted.[3] Following the table are detailed explanations regarding each test configuration.

Configuration	%Change over 3.06	Failure %Change over 3.06	%Change over 4.0 Base	Mb/sec
Base System (BS)	90.37	0.23	n/a	11.07
BS +64MB	89.73	-0.50	-0.59	11.12
BS +192MB	87.15	**-2.24**	0.90	11.24
BS using PCI	156.79	**-2.05**	**22.03**	19.47
BS with no reverse lookups	78.86	**-1.64**	-0.21	10.98
BS with no http caching	84.68	**-0.93**	-1.23	11.10
BS + PCI + MaxReceive	110.37	0.44	**20.83**	19.00
BS + maxReceive=500	88.33	0.27	2.21	10.94
BS + 1p	50.66	**-1.95**	-3.74	10.92
BS on 10mb network	-5.37	-0.35	**-20.26**	8.82
2p full system	84.22	n/a	**26.42**	22.46
BS + 100 rules	16.10	**-47.91**	1.80	10.75
BS + 3p	n/a	n/a	-1.16	11.13
BS with WebNot(1 cat. 1,000 URLS)	n/a	n/a	-2.71	10.88
BS with WebNot(1 cat. 5,000 URLS)	n/a	n/a	-1.48	10.76
BS with WebNot(1 cat. 10,000 URLS)	n/a	n/a	1.20	10.94
BS with WebNot(5 cat. 1,000 URLS)	n/a	n/a	0.57	10.91
4p full system	n/a	n/a	**23.93**	21.42
BS with WebNot(1 cat. 100,000 URLS)	n/a	n/a	1.14	10.93

Table 2. *A summary of configurations tested. Significant changes highlighted. Performance increases are negative numbers in column 2(Failure %Change) and positive numbers in column 3 (%Change over base).*

[2] See Appendix A for an explanation of the NSTL methodology. Also see Performance Analysis and Tuning of Raptor's EagleNT 3.06 Firewall on Compaq Servers (http://www.compaq.com/support/techpubs/whitepapers/278a0497.html).

[3] In the column titled ***Failure %Change over 3.06***, the more negative a number, the better performance it indicates for that configuration. In the column titled ***%Change over Base***, the more positive a number, the better performance it indicates for that configuration.

Base System

The base system consisted of the following elements:

- Compaq ProLiant 5000
- 1-Pentium Pro 200 MHz Processor, 512K cache
- 64 MB RAM
- 100-megabit network
- 2-EISA NetFlex-3 Network Interface Cards
- MaxReceives Buffer for NetFlex-3 cards equals 100
- DNS reverse lookups were ON
- HTTP cache was ON
- Four Firewall rules present (allow inside -> inside, inside -> outside, outside -> server1, outside -> server2 for HTTP and FTP)

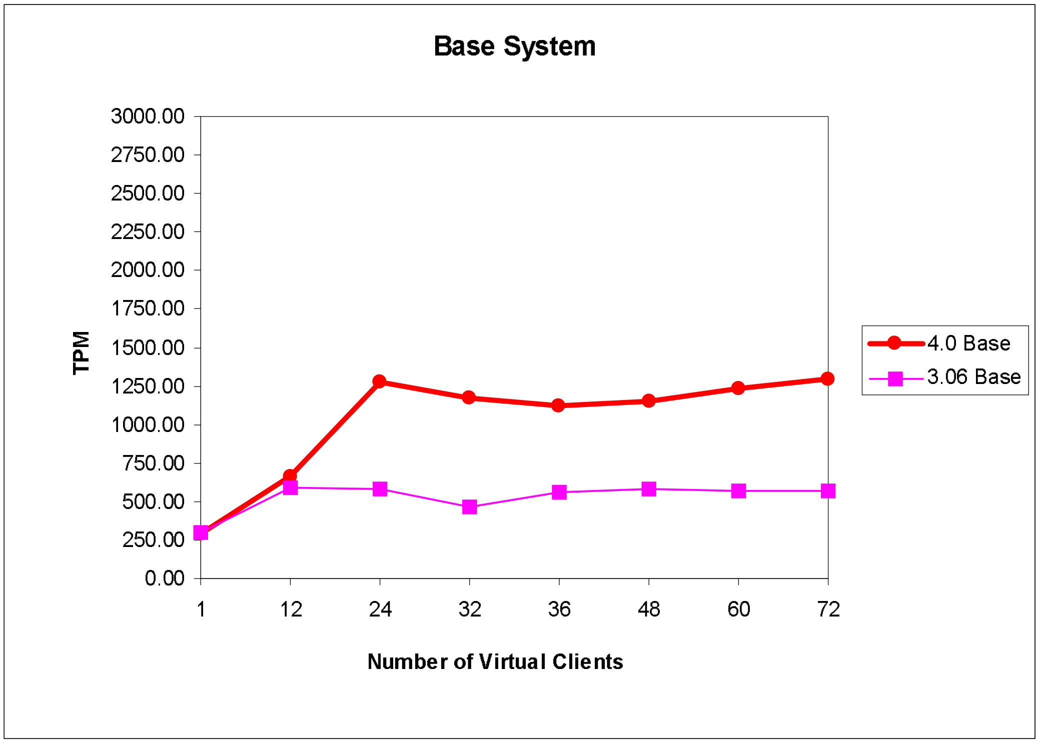

Table 3. *EagleNT 4.0 base system vs. EagleNT 3.06 base system.*

Performance, measured in transactions per minute (TPM), increased 90% from Raptor EagleNT 3.06 to EagleNT 4.0 on the base system. This dramatic performance increase can be attributed to benefits gained from the support of Windows NT 4.0 and Raptor's engineering efforts. Aside from changes made specifically for Windows NT 4.0, Raptor's engineering efforts included a redesign of the high use proxies and improvement of the logging to speed up each transaction.

Adding memory to the base system

Two increased memory configurations were tested. One configuration had 128 megabytes total RAM and the other had 256 megabytes total RAM. ***Neither configuration showed a performance improvement over the base system,*** although using 256 megabytes total RAM reduced the number of failures. Raptor's redesign of the high-use proxies uses memory more efficiently, which accounts for the performance increase when adding memory under EagleNT 3.06, yet not under EagleNT 4.0.

Adding processors to the base system

Four different multi-processor configurations were tested: a two-processor base system, a four-processor base system, a two-processor full system, and a four-processor full system. Adding the appropriate number of processors, then installing the multi-processor HAL creates the multi-processor base system. A full system uses the "best of the best" configurations (256 MB RAM, PCI NICs, MaxReceives Buffer set to 500) in an attempt to maximize throughput.

The performance of the multi-processor base systems compared to that of the base system did not change; however, the performance of the multi-processor full systems improved. The additional processors helped handle the increased throughput caused by the PCI network interface cards. The two-processor total system outperformed the four-processor total system because of the four-processor system's increased overhead.

For EagleNT 4.0, the network is the first bottleneck, processing speed the second; whereas processing speed is the initial bottleneck under EagleNT 3.06.

Changing the NIC BUS from EISA to PCI

By changing the network interface cards from EISA to PCI, an additional performance gain of 22% over the base system was achieved. Furthermore, compared to EagleNT 3.06, TPM increased by over 150% while failures decreased by roughly 2%. For EagleNT 4.0, PCI cards are yielding even greater value in terms of throughput and the ability to handle that throughput efficiently. (See Table 4.)

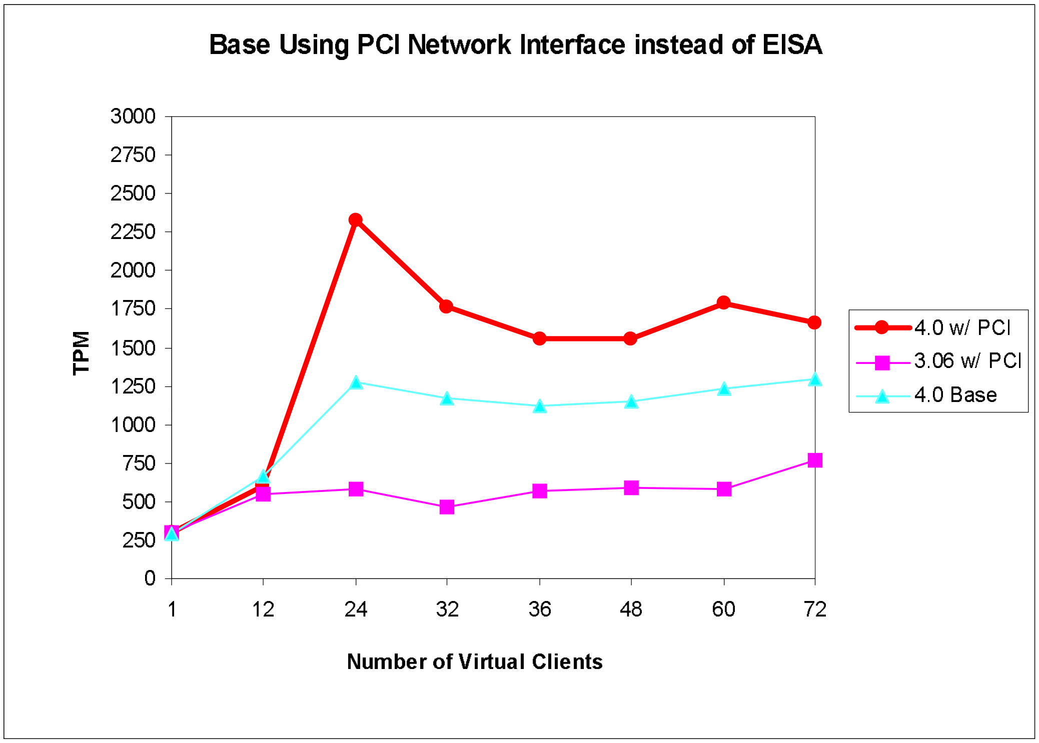

Table 4. *PCI NICs vs. EISA NICs*

Turning off Reverse Lookups / HTTP Caching

A new feature for EagleNT 4.0 allows the user to turn off Reverse Lookups for all daemons. This feature replaces the switches used only on the HTTP daemon in EagleNT 3.06. (httpd.exe –y –z, in %eagledir%\sg\startgw.cmd). To turn off reverse lookups, select Configure Gateway from the Hawk GUI. Select Web->Advanced and clear the Reverse Lookups checkbox. If desired, ***this feature can be utilized with no impact on performance.***

Another switch disables HTTP caching. To disable HTTP caching, edit %eagledir%\sg\startgw.cmd and add –f 0 after httpd.exe, (httpd.exe –f 0). ***Disabling HTTP caching does not affect performance either.***

Adding firewall rules

One hundred firewall rules were created, an increase of ninety-six over the base system, to test their impact on overall performance. ***Increasing the rule base had no impact on performance,*** and compared to the same rule base under EagleNT 3.06, transaction failures decreased by nearly fifty percent!

Running on a 10-megabit Network

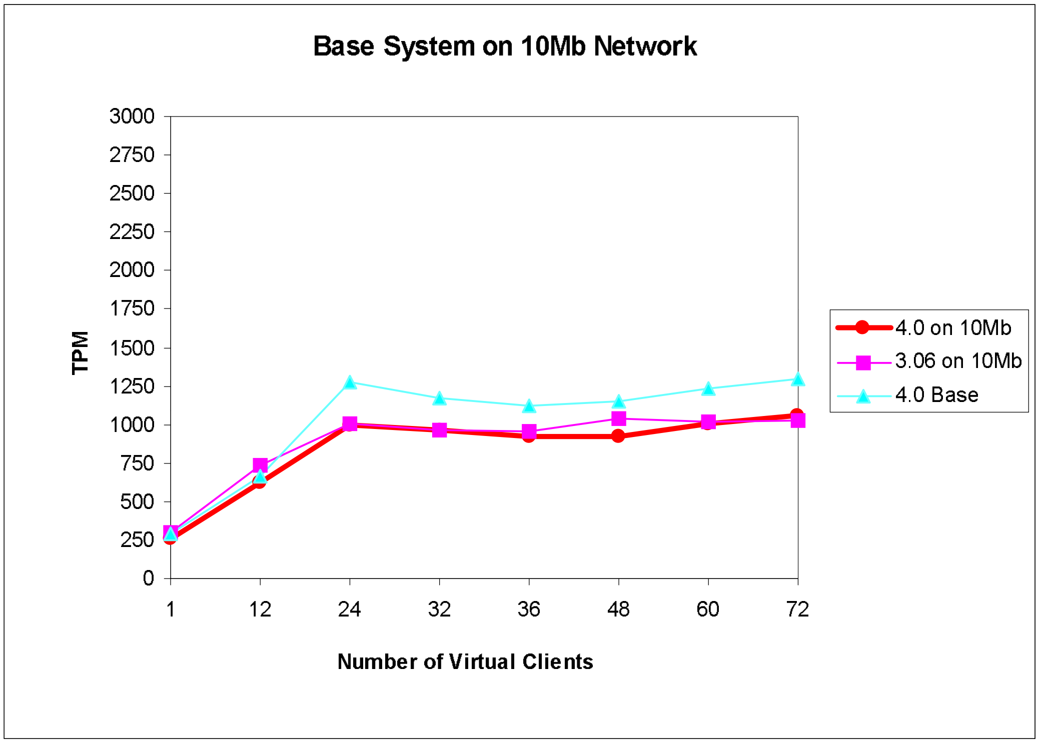

***Table 5**. Running on a 10-megabit Network*

Realizing the increased performance of EagleNT 4.0 on a network with external connections running at speeds greater the ten megabits per second (14 or more T1 lines or a T3 line) entails running on a 100-megabit network. While under EagleNT 3.06 performance degradation on a 10-megabit network was minimal, ***for 4.0 performance degraded by 20%.*** In fact, as Table 5 clearly shows, performance of each version of the Raptor firewall was nearly identical. The network was the performance bottleneck.

Compaq MaxReceives Buffer

The MaxReceives buffer is a user configured registry parameter, which specifies the maximum number of receive lists the driver allocates for receive frames on a Compaq Netelligent 10/100TX controller. To change the parameter make the following registry entry:

```
HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\cpqnf3(#)\Parameters\ MaxReceives = REG DWORD 0x1F4
```

Adding the MaxReceives parameter has no effect on EagleNT 4.0's performance.

Adding WebNot – Objectionable URL blocking

New for EagleNT 4.0 is the ability to block objectionable material (pornography, promotion of gambling, illegal substances, etc.) through a subscription service. Objectionable URLs, categorized by type and alphabetized by IP address and protocol, are listed in a flat file, which is periodically updated by the service. On average, this flat file contains 17,000 URLs. URL blocking is achieved by comparing URLs requested by a client to those listed in the flat file. If a match is found and a corresponding deny rule is set up on the firewall, the URL request is rejected. To test this feature, five WebNot files were created, of varying sizes and numbers of categories. ***None of the WebNot files had any impact on performance, even the one containing 100,000 URLs.***

CONCLUSIONS

The performance of EagleNT 4.0 is vastly superior to that of EagleNT 3.06, as measured by number of transactions handled and number of failures resulting from those transactions. Performance gains can be attributed to improvements in the Raptor firewall and benefits gained from Windows NT 4.0. Enforcing a complex security policy will not affect performance. EagleNT 4.0 allows multiple firewall rules and comprehensive URL blocking without degrading performance. Throughput can be maximized with increased processing power; however, power beyond a single Pentium Pro 200, as found in the Compaq ProLiant 5000, is unnecessary unless used in combination with PCI network interfaces. Regardless of the processor in the firewall machine, performance can be increased by running on a 100-megabit network and by using PCI NIC cards.

APPENDIX - TEST METHODOLOGY

The NSTL testing methodology was designed to test a firewall's ability to route traffic, both HTTP and FTP, under varying client loads. Two measurements are taken: transactions per minute (TPM) and failures. These measurements are taken at various client loads.

NSTL creates "client load" by sending data requests from virtual clients to virtual servers. Virtual clients (and servers) are instances of the client (or server) running on the same physical machine under different names. Version 1.0 of the NSTL benchmark uses twelve physical machines: eight clients, three servers, and the firewall (See Table 6). Each physical server runs two virtual servers. Virtual clients are distributed among the physical clients by a control machine. The control has an interface to each network. For each test discussed in this paper, performance was measured for 1, 12, 24, 32, 36, 48, 60, and 72 virtual clients.

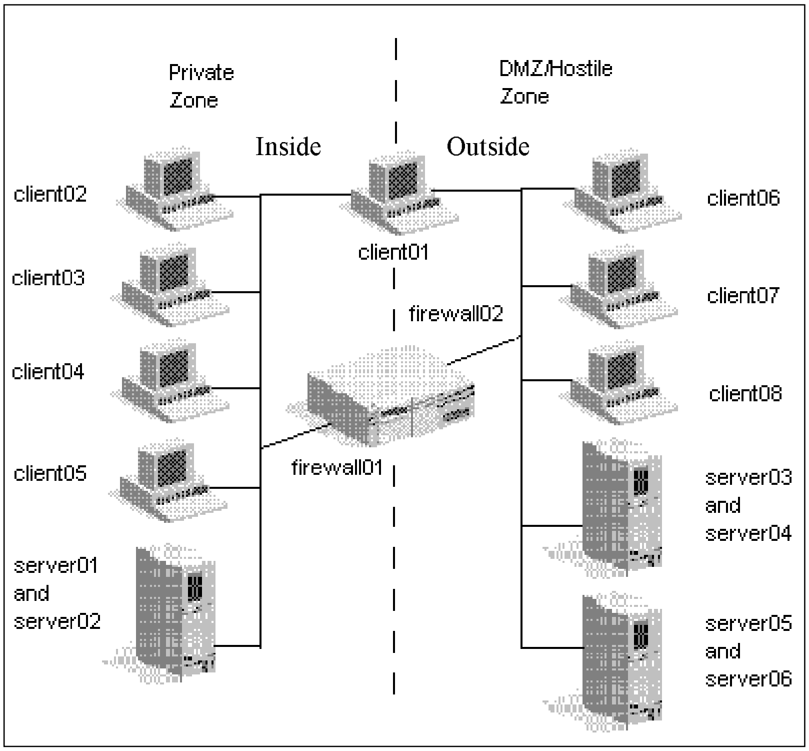

Table 6. The test bed.

Clients in the private zone request data from servers in the private zone and the DMZ/Hostile zone; however, most of the requests are for servers in the DMZ/Hostile zone. The same is true for clients in the DMZ/Hostile zone. The majority of their requests are for servers in the private zone. Table 7 shows the exact percentage of requests taken by each server in the test bed. Table 8 shows the percentage of requests by protocol.

Clients	Server01	Server02	Server03	Server04	Server05	Server06
Client01 - 05	2.4%	2.4%	23.8%	23.8%	23.8%	23.8%
Client06 - 08	40%	40%	5%	5%	5%	5%

Table 7. Server hits by client.

Servers	% FTP Requests	% HTTP Requests
Servers 01, 03, 05	10	90
Servers 02, 04, 06	90	10

Table 8. Protocol percents.

Each machine in the test bed (except the firewall) was a Compaq ProLiant 2000 with two Pentium 90 processors and 32 megabytes RAM. The control client had an additional 32 megabytes of RAM. The client machines were loaded with Windows NT 4.0 Workstation and Service Pack 2. The server machines were running Windows NT Server, Version 4.0, Service Pack 2. Microsoft Internet Information Server, version 3.0 was used as the web server.