WHITE PAPER

May 1998

Internet Solutions
Business Unit

Compaq Computer
Corporation

CONTENTS

Executive Summary 3

Introduction 4

NSTL Test Suite 4

Individual Results 6

Conclusion 11

Appendix 12

Compaq Performance Testing of AXENT Raptor Firewall 5.0 for NT

Compaq and Raptor, now a Division of AXENT Technologies, have partnered to deliver world-class Internet and intranet security on Compaq servers in an easy-to-configure, easy-to-use way. One facet of this partnership is the performance testing of AXENT's products on Compaq hardware. The results of these tests validate AXENT's past development and suggest areas for further enhancement. Compaq has done performance testing on Raptor EagleNT 4.0 (see http://www.compaq.com/support/techpubs/whitepapers/247a0897.html) and Raptor EagleNT 3.06 (see http://www.compaq.com/support/techpubs/whitepapers/278a0497.html). The current paper presents the results of Compaq's performance tests on the latest version, Raptor Firewall for NT.

Note: While this performance paper was being prepared, AXENT issued a point release of the Raptor Firewall, making the latest version 5.01. This release fixes bugs and introduces a smoother upgrade path to the latest version. It also introduces Finjan SurfinGate Lite for JAVA filtering. These changes should not affect the Raptor Firewall performance results documented here.

COMPAQ

NOTICE

The information in this publication is subject to change without notice and is provided "AS IS" WITHOUT WARRANTY OF ANY KIND. THE ENTIRE RISK ARISING OUT OF THE USE OF THIS INFORMATION REMAINS WITH RECIPIENT. IN NO EVENT SHALL COMPAQ BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION), EVEN IF COMPAQ HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The limited warranties for Compaq products are exclusively set forth in the documentation accompanying such products. Nothing herein should be construed as constituting a further or additional warranty.

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 is registered with the United States Patent and Trademark Office.

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

Eagle, EagleNT 3.06, EagleNT 4.0, EagleNT 5.0 and Raptor are trademarks and/or registered trademarks of Raptor Systems Inc. Raptor Systems is a division of AXENT Technologies.

Finjan and SurfinGate Lite are trademarks and/or registered trademarks of Finjan Software Ltd.

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 Compaq using licensed testing products from NSTL. NSTL does not guarantee the accuracy, adequacy, or completeness of the services provided in the connection with Compaq'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 EXPRESSED OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULARPURPOSE OR USE WITH RESPECT TO THE SERVICES AND/OR RESULTS TEREROF, OR ANY INFORMATION OR DATA INCLUDED THEREIN.

Compaq Performance Testing of AXENT Raptor Firewall 5.0 for NT
Second Edition (May 1998)
ECG012/0598

EXECUTIVE SUMMARY

This paper used the NSTL software benchmark methodology to test the performance of the AXENT Raptor Firewall 5.0 for NT. Testing included the following actions involving hardware and software configuration:

- increasing memory
- adding additional processors
- changing the NIC type
- using network switches instead of hubs
- using the new Fastpath option
- creating large numbers of firewall rules
- blocking large numbers of objectionable URLs
- reducing the amount of logging

The results obtained from testing led to the following conclusions:

- A high mark of 50 megabits per second (mbps) was achieved on a Compaq ProLiant 1600 server with a single 400-MHz processor and the AXENT Raptor Firewall with the Fastpath option maximized.
  - Even the lowest measured throughput, approximately 20 mbps, is enough to support thirteen T1 (1.54-mbps) lines, while the maximum measured throughput can support thirty-one T1 lines, or a T3 line.
- Data throughput on the AXENT Raptor Firewall consistently increases when processors are added. Throughput also increases as processor speed increases.
- Replacing 100-mbps network hubs with 100-mbps network switches will not increase data throughput over the network.
- Performance of Network Interface Cards (NICs) of different manufacturers does vary.
- Additional memory does not affect performance. 64 MB of RAM is adequate to support the firewall.
- The WebNOT, NewsNOT, and reduced logging features do not affect performance.
- A high number of firewall rules (up to 100 were tested) will not affect performance either.

INTRODUCTION

Compaq's performance testing provides anyone who has deployed or is considering deploying a firewall with the means to decide what firewall configurations are appropriate for their business needs. Furthermore, it validates AXENT's past development efforts, and suggests areas for future development. Compaq's performance analysis includes both hardware and software (firewall) configurations.

The performance tests were recorded using the National Software Testing Laboratories (NSTL) Firewall Performance Benchmark, Version 97-009. This is an update to the version used in the previous tests of AXENT Raptor Firewall. An overview of the test network is given in the "NSTL Test Suite" section of this paper. Before any tests were run on the firewall, diagnostics were performed on the test network. From these tests, valuable insight was gained into improving overall network performance. These findings are summarized in the appendix.

As Compaq's testing of AXENT Raptor Firewall continues, the test configurations are modified based on past results and new features in the firewall software. Several different hardware platforms were tested in support of the recently announced Compaq ProSignia and ProLiant Firewall Servers. New features of AXENT Raptor Firewall include improved multiprocessor capabilities, Fastpath (a means of enabling packet filtering where appropriate), NewsNOT (a content blocker for news groups similar to WebNOT), and a reduced logging feature.

While this paper was being prepared, AXENT issued a point release of the Raptor Firewall, making the latest Version 5.01. This release fixes bugs and introduces a smoother upgrade path to the latest version. It also introduces Finjan SurfinGate Lite for JAVA filtering. These changes should not affect the AXENT Raptor Firewall performance results documented here.

NSTL TEST SUITE

Firewall performance testing is done to achieve a maximum throughput number under controlled conditions. The testing helps reveal how much traffic a firewall can handle, what parameters affect throughput, and what opportunities exist for improving the firewall's performance. Performance testing of AXENT Raptor Firewall was done using an updated version of the NSTL Firewall Performance Benchmark (97-009). Before any performance testing occurred, the benchmark itself was tested to determine ideal client loads, to test variability, and to maximize throughput.

Figure 1 shows the test bed used by the NSTL benchmark. The test bed is divided into three networks or zones: the private zone (192.168.1.0), the DMZ (192.168.2.0), and the hostile/Internet zone (192.168.3.0). The private zone contains one client. This client sends requests to two servers, a server in the DMZ and a server in the hostile zone. The server in the DMZ receives thirty percent of the requests while the server in the hostile zone receives the remaining seventy percent. Another client is located in the hostile zone. This client sends requests solely to the server in the DMZ. Each physical client machine spawns multiple virtual clients that send an 80/20 mix of HTTP and FTP requests.

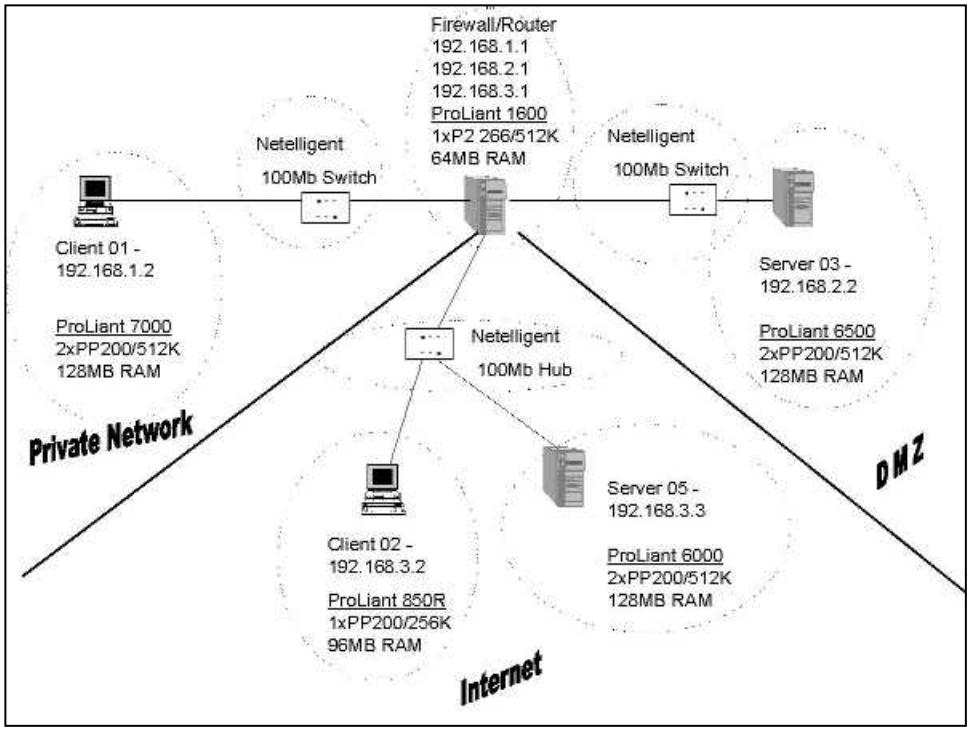

Figure 1.The NSTL test bed

The maximum number of virtual clients that a physical client could spawn without error was twenty; however, this enabled generation of up to eighty mbps of traffic (TCP/IP headers are not included in the overall throughput numbers). This level of throughput was more than enough to saturate the network and simulate hundreds of simultaneous users under real-world conditions. Running more than twenty virtual clients did not increase the network traffic, it increased only the number of errors due to timeouts. This result led to the decision to run virtual client loads of four, eight, twelve, sixteen, and twenty for each test configuration.

For any given test, throughput numbers will vary. Ten identical tests revealed a standard deviation of .89 (3.52%). Assuming a normal distribution, sixty-eight percent of the data should be in a range one standard deviation away from the average, and ninety-five percent of the data should lie within two standard deviations. Therefore, to attribute a performance difference to a change in configuration, a change of greater than seven percent would have to be observed.

INDIVIDUAL RESULTS

As noted earlier, the performance tests of AXENT Raptor Firewall were done using the NSTL Firewall Benchmark tool Version 97-009. However, a control was first established using a minimum configuration. This configuration is defined in the "Base System" section of this paper. Throughput data was collected for the base system. Subsequent tests changed one configuration parameter of the base system, and throughput data was collected again. This data was then compared to the base system to determine the effect of the configuration change. A summary of the tests performed appears in Table 1, while Table 2 shows the results of tests run on completely different server platforms (or base systems). The additional platforms tested were the ProLiant 850R, ProLiant 3000, ProLiant 6500, and ProSignia 200. Each of these systems had 64 MB of RAM and three Intel EtherExpress Pro Network Adapters, except the ProLiant 850R, which used the embedded Netelligent NIC and two other Netelligent NICs. All NICs had 100-Mb capability.

TABLE 1. SUMMARY OF CONFIGURATION CHANGES TO THE PROLIANT 1600 BASE SYSTEM

Configuration	Virtual Client Load (Mb/sec) 4	8	12	16	20	avg. Mb/sec	% Change over Base
Base System (BS) ProLiant 1600	24.76	25.63	25.32	25.43	25.51	**25.33**	
BS + 64MB RAM	9.48	27.82	25.41	26.43	27.27	**26.73**	**5.54**
BS with Hubs	23.79	25.44	25.97	25.15	26.20	**25.31**	**-0.08**
BS + 1p	27.14	35.16	37.17	36.40	35.51	**34.28**	**35.32 ***
BS + 2way Fastpath	27.96	31.91	33.39	33.42	33.95	**32.13**	**26.83 ***
BS + 1way Fastpath	26.25	27.43	27.37	30.57	28.93	**28.11**	**10.98 ***
BS, reduced logging	25.01	26.61	26.56	26.78	26.13	**26.22**	**3.51**
BS, 100 rules	24.65	25.67	25.75	25.54	26.70	**25.66**	**1.31**
BS, content blocking	24.30	25.00	25.90	26.07	26.97	**25.65**	**1.26**

* These figures denote a significant (> 7%) change.

TABLE 2. SUMMARY OF DIFFERENT HOST SYSTEMS

Configuration	Virtual Client Load (Mb/sec) 4	8	12	16	20	avg. Mb/sec	% Change over 1P
ProLiant 850R, 1*Pentium Pro 200MHz	19.23	20.21	20.19	20.93	21.02	**20.32**	*n/a*
ProLiant 850R, 2*Pentium Pro 200MHz	20.85	23.22	24.17	20.23	23.12	**22.32**	**9.87 ***
ProLiant 6500, 1*Pentium Pro 200MHz	22.79	23.99	24.12	24.09	25.01	**24.00**	*n/a*
ProLiant 6500, 2*Pentium Pro 200MHz	27.51	30.26	30.80	31.21	31.54	**30.27**	**26.10 ***
ProLiant 6500, 4*Pentium Pro 200MHz	30.93	34.00	37.84	38.47	38.36	**35.92**	**49.67 ***
ProSignia 200, 1*Pentium II 233MHz	21.27	23.17	22.62	21.68	21.42	**22.03**	*n/a*
ProLiant 3000, 1*Pentium II 300MHz	25.48	26.18	28.10	27.36	27.21	**26.87**	*n/a*
ProLiant 3000, 2*Pentium II 300MHz	31.37	34.19	35.85	36.62	35.47	**34.70**	**29.15 ***
ProLiant 1600, 1*Pentium II 400MHz	31.92	36.06	32.30	37.18	35.54	**34.60**	*n/a*
ProLiant 1600, 1*Pentium II 400MHz (Bi-Directional Fastpath ON)	41.88	47.93	47.68	50.57	49.41	**47.50**	*n/a*

* Note that the percent change column compares the effect of additional processors added to the same machine. It does not compare it to the ProLiant 1600, the base system in Table 1.

Base System

The base system (the host for the firewall system) consisted of the following elements:

- Compaq ProLiant 1600
- One Intel Pentium II, 266-MHz Processor, 512K cache
- 64 MB RAM
- 100-mbps switched network
- Three PCI Intel EtherExpress Pro NICs (100-mbps)
- The following six firewall rules
  - Allow FTP traffic from network 192.168.1.0 to network 192.168.2.0
  - Allow HTTP traffic from network 192.168.1.0 to network 192.168.2.0
  - Allow FTP traffic from network 192.168.1.0 to network 192.168.3.0
  - Allow HTTP traffic from network 192.168.1.0 to network 192.168.3.0
  - Allow FTP traffic from network 192.168.3.0 to network 192.168.2.0
  - Allow HTTP traffic from network 192.168.3.0 to network 192.168.2.0
- For all firewall rules, the Fastpath and reduced logging options were not selected
- The content blocking database (WebNOT and NewsNOT) was not installed

The performance tests were first run on the base system. Subsequent tests were then compared to the base system to see if a performance change could be attributed to the configuration change. As mentioned in the "NSTL Test Suite" section of this paper, a seven percent change was necessary to attribute the performance change to the new configuration. A summary of the results is found in Table 1.

Adding Memory to the Base System

To test the effect of additional memory on firewall throughput, an additional 64 MB of RAM was added to the base system. This gave the firewall server a total of 128 MB of RAM.

The additional memory did not affect performance. This is consistent with the performance tests on the earlier versions of AXENT Raptor Firewall.

Replacing Network Switches with Hubs

This configuration replaced the 100-mbps switches (see Figure 1) with 100-mbps hubs. Hubs and switches performed equally well with a firewall installed on the network. This is in stark contrast to the results when a router is used rather than a firewall.

At the high throughput levels (70+ mbps) allowed by a router, the switch reduces the number of packet collisions on the network, yielding higher throughput. With a firewall present, throughput levels are reduced to the extent that switching technology provides no further benefit over hubs.

Adding Processors to the Base System

Data throughput on AXENT Raptor Firewall consistently increases when more processors are added. The results are summarized in Table 3. As the table shows, not only was an additional 266-MHz processor tested in the ProLiant 1600, but also different processor configurations varying in speed from 200 MHz to 400 MHz were tested in several Compaq servers.

TABLE 3. SUMMARY OF PROCESSOR CONFIGURATIONS

		Number of Processors Average Mb/sec (% Change)		
Host Machine	**Processor Speed**	**1**	**2**	**4**
ProLiant 6500	200-MHz	24.00	30.27 (+18.5%)	35.92 (+49.5%)
ProLiant 850R	200-MHz	20.32	22.32 (+9.8%)	N/A
ProSignia 200	233-MHz	22.03	N/A	N/A
ProLiant 1600	266-MHz	25.33	34.28 (+35.3%)	N/A
ProLiant 3000	300-MHz	26.87	34.70 (+29.1%)	N/A
ProLiant 1600	400-MHz	34.60	N/A	N/A

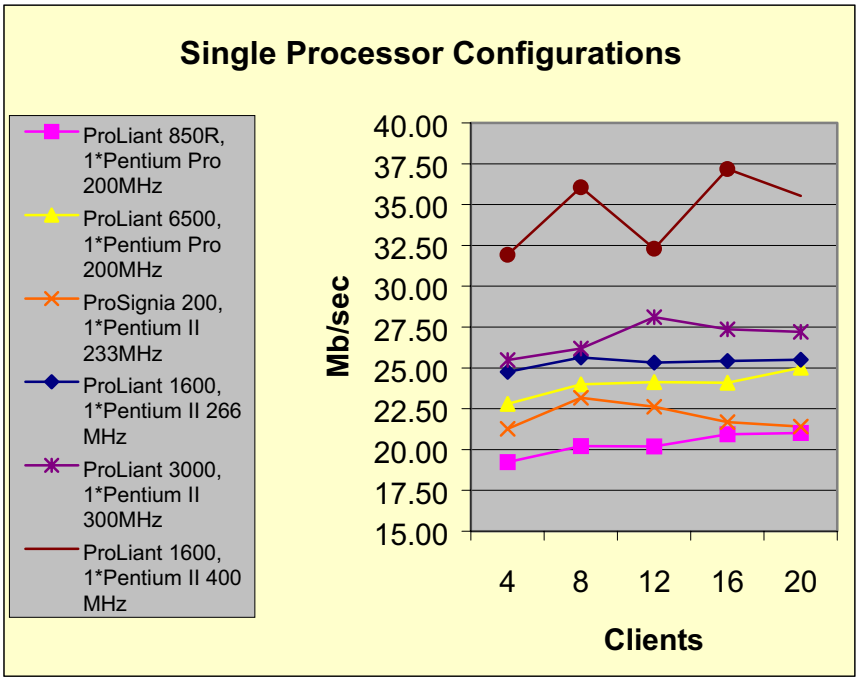

Figure 2. Comparison of single-processor configurations

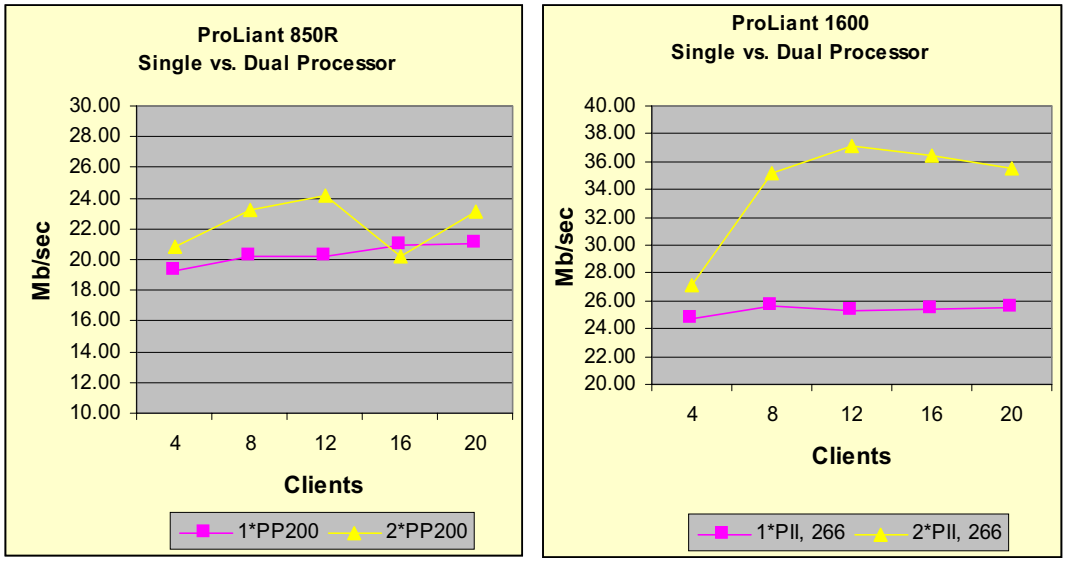

Figure 3. ProLiant 850R and 1600, single versus dual processor

Enabling the Fastpath Option

Fastpath is a new feature of AXENT Raptor Firewall that allows it to act on packets at the network level (like a packet filter) rather than at the application level. This option can be applied on a per-rule basis and dramatically improves data throughput.

When Fastpath was applied for packets travelling from the inside network to the outside network (labeled "One way" in Figure 4), throughput increased eleven percent. When Fastpath was applied for all traffic, throughput increased by 26.8 percent. In fact, data throughput of fifty mbps was achieved when bi-directional Fastpath was applied to the ProLiant 1600 with a single 400-MHz processor ("bi-directional" means data travelling into and out of the protected network).

The increased throughput mentioned above comes at the cost of decreased security. A warning is displayed when the Fastpath option is selected, and the option should be used only after careful consideration of the risks. It is recommended that the Fastpath option not be used for incoming traffic from the Internet.

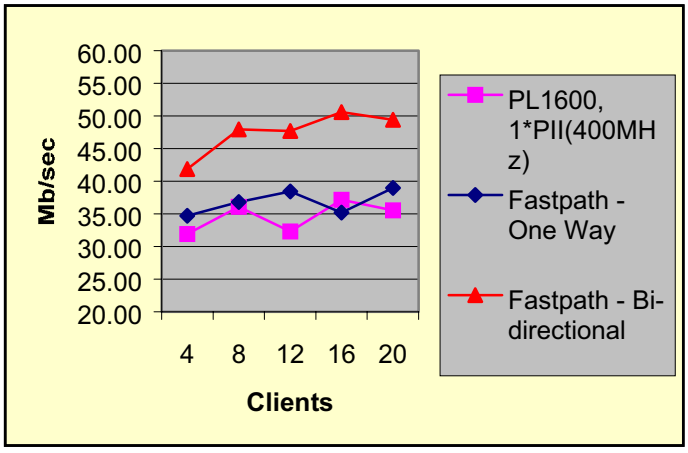

Figure 4. Fastpath option enabled

Content Blocking

The ability to block objectionable news groups (NewsNOT) is a new feature in AXENT Raptor Firewall 5.0 for NT. It adds to the existing capability provided by WebNOT to block objectionable material such as pornography, promotion of gambling, and illegal substances. Both features are available through a subscription service. Objectionable URLs, categorized by type and alphabetized by IP address and protocol, are listed in a flat file that is periodically updated by the service. 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. The same file contains URLs for both objectionable websites and news groups. Consistent with the Raptor EagleNT 4.0 tests, this feature does not affect the performance of the firewall.

Reduced Logging and a High Number of Firewall Rules

In the administration of a security policy, one way to ease the maintenance of a firewall is by creating many simple rules. Using the base system as an example, separate rules have been created for each allowed protocol. In a complex network environment, many protocols must be supported; therefore, a high number of rules will be created. To test the impact of a large number of firewall rules on performance, one hundred firewall rules were created. No performance impact was noted at this number of firewall rules.

A second way to ease firewall maintenance is by reducing the size of the logs. AXENT Raptor Firewall allows logging to be turned off on a per-rule basis. Thus, where a business case exists, superfluous information need not be logged. One might think that reducing the amount of logging would reduce the overall amount of work the firewall is doing per transaction, and that performance would improve. However, the performance tests did not support this hypothesis. Reduced logging did not affect performance in any way.

CONCLUSION

Raptor continues to make improvements in its firewall software. The latest version, 5.0, has improved overall throughput to over 20 mbps in all tested configurations, and a fully maximized firewall configuration can yield up to 50 mbps. Enforcing a complex security policy will not affect performance. AXENT Raptor Firewall 5.0 for NT allows multiple firewall rules and comprehensive content blocking without degrading performance. Further flexibility is gained with the ability to configure the firewall as a packet filter, and by allowing reduced logging. The firewall scales well with added processing power. In all cases, adding an additional processor will improve performance.

APPENDIX

Network Optimization Tips

Before the NSTL benchmark was run, the test network was optimized for performance. The machine that would host the firewall was first configured as a router. Every route in the network was tested for maximum throughput. A program that sent multiple URL requests was used to obtain transfer times. In some cases the transfer times varied by over 20 mbps. The test network was optimized in the following ways:

- The latest service pack was applied to the operating system of each machine on the test network. In this case, Service Pack 3 for Microsoft Windows NT 4.0 was applied to correct some TCP/IP errors. These errors had previously been addressed in hot fixes.
- The latest NIC drivers were installed.
- Performance of network interface cards (NICs) of different manufacturers does vary. Changing NICs could increase performance.
- Faulty CAT 5 network cables and NICs were replaced. These replacements increased performance by 20 mbps in some cases. The cables that were replaced were functional, but due to faulty construction, age, and other factors, introduced high levels of errors that caused a reduction in throughput.
- Network switches, instead of hubs, were used to reduce the number of packet collisions occurring on the network.
- The Web servers were given enough memory and processing power to ensure that they were not a throughput bottleneck.
- HTTP and FTP logging was turned off on the servers. The firewall performed the logging of each transaction, and this reduced the number of FTP timeouts. Again, this ensured that the Web servers were not a bottleneck.
- The NICs were set for automatic detection of network speed and duplex mode.