COMPAQ
White Paper

September 1998
ECG045/0998

Prepared by Internet Solutions
Business Unit

Compaq Computer Corporation

Compaq Performance Testing of AXENT Raptor Firewall Virtual Private Network Implementation

Contents

Abstract: The Internet has become the de facto standard for today’s data communication; however, its open architecture does not inherently provide for secure transmission of that data. Virtual Private Networking is gaining popularity as the means for securing this data communication. As with any security measure, a Virtual Private Network (VPN) impacts performance negatively as the level of security increases. This paper examines the VPN protocols offered by the AXENT Raptor Firewall 5.0 for NT, their performance differences, the effect of processor speed on performance, and the protocols' performance as related to file size (and ultimately packet size). The performance results give the firewall administrator critical facts which allow a more informed performance-versus-security decision.

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, ProLiant, and ProSignia are registered with the United States Patent and Trademark Office.

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

Pentium, Pentium II, and Pentium Pro are trademarks and/or registered trademarks of Intel Corporation.

Raptor is a trademark and/or registered trademark of Raptor Systems Inc. Raptor Systems is a division of AXENT Technologies.

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 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 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.

Compaq Performance Testing of AXENT Raptor Firewall Virtual Private Network Implementation
White Paper prepared by Internet Solutions Business Unit

First Edition (September 1998)
Document Number ECG045/0998

Introduction

This paper documents the performance differences exhibited by various Virtual Private Network (VPN) configurations between two subnets. These subnets could represent remote sites or different businesses which are connected to the Internet and communicate via a VPN. The following factors were tested with different VPN configurations:

- Transmission/management protocol, including IP Security (IPSec), Internet Security Association and Key Management Protocol (ISAKMP), and Software IP Encryption (swIPe)
- Encryption algorithm, including Data Encryption Standard (DES), Triple DES, and RC2
- Authentication algorithm, including Message Digest 5 (MD5) and Secure Hash Algorithm-1 (SHA-1)

To test these factors, the National Software Testing Lab's (NSTL) Firewall Benchmark Version 97-009 was used to generate traffic between a client and a Web server. This traffic passed through two Compaq ProSignia 200 Firewall Servers running the AXENT Raptor Firewall 5.0 for NT VPN implementation. To test the effect of processor speed at the firewall server, the Compaq ProSignia 200 Firewall Servers were replaced with both Compaq ProLiant 1600 Firewall Servers and Compaq ProLiant 1850R Firewall Servers, boosting the processor speed from 266 MHz to 400 MHz in each case.

The tests revealed the following:

- VPN tunnels can decrease throughput by up to 40% for large files. Throughput for small and medium files is not significantly reduced by tunneling.
- Encryption and authentication will further diminish throughput. Throughput degradation is a function of file size.
- Despite these reductions, throughput is sufficient to satisfy between three and six T1 lines -- ample enough to meet the demands of most companies.
- Using the DES algorithm in a tunnel reduces throughput by 30% compared to a tunnel with no encryption; using Triple DES reduces throughput by 52%, and using RC2-40 reduces throughput by 55%, compared to a tunnel with no encryption. All comparisons are based on large files.
- Faster processors will increase throughput when using a VPN. A 400-MHz processor increased throughput by anywhere from 20-40% over a 266-MHz processor.
- The ISAKMP/Oakley protocol, which dynamically creates IPSec tunnels and manages keys for ease of administration, is 14% faster for DES using large files than manual IPSec. A faster processor does not improve ISAKMP throughput as significantly as it does IPSec.
- Using MD5 authentication is comparable in throughput to using SHA-1.
- Replay protection can be implemented without performance degradation.

Note: With Version 5.0, the Raptor Firewall does not implement compression of the data being transmitted through the VPN tunnel.

VPN Overview

The intent of this section is not to fully explain VPN technology, but instead to provide a baseline of information regarding VPNs as is pertinent to performance testing. For further details on VPN technology, please refer to the following documents:

AXENT Raptor Firewall Reference Guide (Chapter 10, "VPN Tunnels")

AXENT Raptor Firewall Configuration Guide (Chapter 11, "Configuring Secure Tunnels" and Appendix A, "Sample Secure Tunnel Configurations")

http://www.compaq.com/activeanswers: AXENT Raptor Firewall 5.0 for NT Planning, Deployment, and Operations Guide (Appendix I, "Virtual Private Network Primer and Example Setup"

Note: http://www.compaq.com/activeanswers is a subscription site.

The term "virtual private network" implies that a network exists, not physically, but virtually, and is accessible to individuals with the proper credentials. The network is the Internet, and its access and virtual nature are controlled by the VPN solution. Technically, this is accomplished by taking the original data packets and encapsulating them within additional packets along with security information. This security information includes data integrity checksums and optional encryption.

Standards are evolving for VPN encryption and authentication. The two most common standards or protocols are IPSec[1] and ISAKMP[2]. In addition, AXENT Raptor Firewall 5.0 for NT provides a proprietary swIPe protocol. These protocols utilize standard encryption (DES, Triple DES, and RC2), authentication algorithms (MD5, SHA-1), and provide advanced features such as transport mode and replay protection.

Authentication Header (AH)[3]. This header conveys the authentication information of the IP datagram (packet). The authentication information is calculated using the fields of the datagram that do not change during transmit.

DES[3]. DES (Data Encryption Standard) is a National Institute of Standards and Technology (NIST)-standard secret-key cryptography method that uses a 56-bit key. DES is based on an IBM algorithm that was further developed by the U.S. National Security Agency. DES decryption is very fast and widely used. The secret key may be kept a total secret and used repeatedly. Alternatively, a key can be randomly generated for each session, in which case the new key is transmitted to the recipient using a public key cryptography method such as RSA.

Triple DES[3.] Triple DES is an enhancement to DES that provides considerably more security than standard DES. There are several Triple DES methods. EEE3 uses three keys and encrypts three times. EDE3 uses three keys to encrypt, decrypt and encrypt again. EEE2 and EDE2 are similar to EEE3 and EDE3, except that only two keys are used, and the first and third operations use the same key.

RC2[3]. RC2 is one of the secret key block cryptographic methods developed by RSA Data Security, Inc., Redwood City, CA. (The Raptor Firewall implements a 40-bit key.) RSA Data Security is more widely known for its RSA public key method.

[1] (IP SECurity) A security protocol from the IETF that provides authentication and encryption over the Internet. IPSec works at layer 3 and is supported by IPv6.

[2] (Internet Security Association and Key Management Protocol) A security protocol that dynamically creates IPSec tunnels for ease of administration.

[3] Definition obtained from CMPnet (Techweb) TechEncyclopedia at http://www.techweb.com/encyclopedia/. EEE is "Encryption, Encryption, Encryption;" EDE is "Encryption, Decryption, Encryption."

MD5[3]. MD5 (Message Digest 5) is a popular one-way hash function developed by Ronald Rivest (the "R" in RSA) which is used to create a message digest for digital signatures.

SHA-1[4] . SHA-1 (Secure Hash Algorithm-1) is a popular one-way hash algorithm used to create digital signatures. SHA was developed by the NIST, and SHA-1 is a revision of the standard released in 1994. SHA-1 is similar to MD5, but is slightly slower and more secure.

Tunnel mode. Tunnel mode is the most popular implementation of most VPNs. Both the header and data portions of each packet are encapsulated.

Transport mode. Transport mode is an alternative to tunnel mode. Instead of encapsulating the data and header portions of the packet, transport mode encapsulates only the data portion, reusing the header. This mode is used less often than tunnel mode.

Replay protection. Replay protection prevents retransmission of valid packets which may have been captured for unauthorized purposes.

As some of these definitions imply, performance differences exist between the above options. Those differences are illustrated in the "Test Results" section of this paper.

Test Method

The performance numbers reported in this paper were obtained by generating specific amounts of traffic over various VPN configurations and measuring corresponding throughput values. The traffic was generated and recorded by National Software Testing Labs (NSTL) Firewall Benchmark, Version 97-009. The test network was composed of four machines: a client, two firewalls, and a server. See Figure 1. These four machines created two private networks (192.168.1.0 and 192.168.3.0), and a public network which represented the Internet.

[4] Definition obtained from CMPnet (Techweb) TechEncyclopedia at http://www.techweb.com/encyclopedia/.

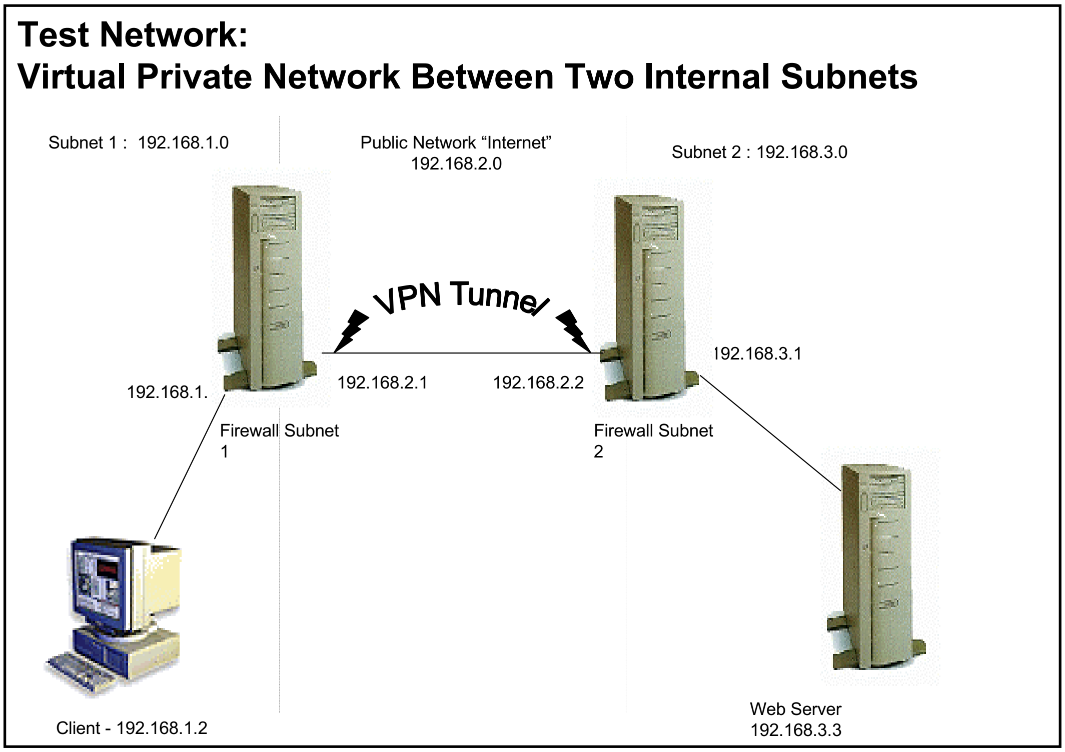

Figure 1. The test network.

The firewall machines were Compaq ProSignia 200 Firewall Servers, each with single Pentium II 266-MHz processors and 64 MB RAM. The client and Web server were both ProLiant 6000 servers with dual Pentium Pro 200-MHz processors and 128 MB RAM. All firewall and client machines ran Microsoft Windows NT 4.0 with Service Pack 3.

The battery of tests run for each VPN configuration included HTTP and FTP requests (from the client to the server) for three different file sizes: small, medium, and large. See Table 1. Eighty percent of the requests were HTTP, the remaining twenty percent FTP. The 100-Mb Ethernet network became saturated when requests came from twenty virtual clients (spawned by the client, 192.168.1.2). Therefore, requests from 4, 8, 12, 16, and 20 virtual clients were made for each battery to represent varying client loads. In total, fifteen tests were run for each VPN configuration.

Raptor Firewall's swIPe protocol was used as a reference point for all other VPN configurations. It was selected because it allowed a tunnel to exist between the firewalls on each subnet, without requiring authentication headers or data encryption. By comparing throughput values to those obtained with swIPe, the performance degradation caused by either encryption or authentication headers became apparent.

Before any data comparisons were made between the various VPN configurations, data was gathered about the test tool itself. Ten consecutive test batteries were run, revealing standard deviations in throughput of 2.45% for large files, 6.06% for medium-sized files, and 13.74% for small files. This means that to attribute a performance change to the variable being examined, it must create a percent change greater than 4.9% for large files[4], greater than 12.12% for medium sized files, and 27.48% for small files.

	HTTP (80%)	FTP (20%)
Small	1,023 bytes	10,230 bytes
Medium	10,230 bytes	95,040 bytes
Large	95,040 bytes	1,013,760 bytes

Table 1. File sizes of client requests

Test Results

As mentioned previously, each VPN configuration tested the throughput differences between small, medium, and large files. The premise was that different-sized files would create different numbers and sizes of packets. Larger files have a higher throughput potential because there is less setup overhead per megabyte transferred. Because of their higher throughput potential, the larger files were more greatly affected when transmitted over the VPN.

The processing overhead of small files was more significant than that of the authentication or encryption method employed by the VPN configuration; yet, when client load became significantly large (16-20 virtual clients) encryption and authentication processing time did become a factor. In other words, throughput for small files was the same with or without a VPN tunnel.

VPN versus No VPN

The review of the results of the performance tests will begin by showing the throughput differences over a network with and without VPN tunnels . Large files were the only files to show significant throughput degradation, a significant 40%. Medium and small-sized files showed insignificant degradation. Results are illustrated in Figure 2.

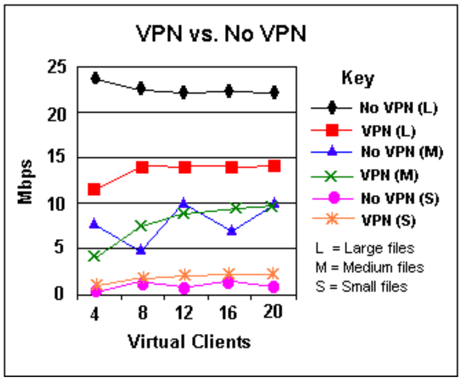

Figure 2. Throughput (Mbps) on a network with and without VPN tunnels

From this point on, throughput comparisons will be made using the VPN configurations (Large, Medium and Small) labeled "VPN" in Figure 2. It is the Raptor Firewall swIPe protocol with no

[4] Assuming a normal distribution, 68% of the data should be in a range one standard deviation away from the average, and 95% of the data should lie within two standard deviations.

authentication and no encryption, and will be referred to as the “base.” Table 2 shows the base numbers for a VPN tunnel without authentication or encryption.

Base Throughput (Mbps) for Small, Medium and Large Files			
Number of Clients	Large Files	Medium Files	Small Files
4	10.95	4.12	1.01
8	13.96	7.12	1.48
12	14.31	8.94	1.89
16	13.94	9.56	2.13
20	14.19	10.06	2.27

Table 2. Base throughput in megabits per second for small, medium, and large files (VPN tunnel without authentication and encryption)

Encryption

Three different encryption algorithms were examined in the performance tests: DES, Triple DES, and RC2-40. DES and Triple DES were tested using IPSec and ISAKMP. For IPSec, encryption was tested with and without authentication headers. The DES algorithm reduced throughput approximately 30% from the base, Triple DES 52%, and RC2-40 55% for large files. Larger files saw greater performance degradation than medium-sized files in all cases. Figure 3 shows the performance of No VPN, VPN (with swIPe), and the three encryption algorithms using large files. RC2 40-bit encryption is not considered very secure; therefore, subsequent comparisons will focus on DES and Triple DES encryption. Results comparing DES and Triple DES are summarized in Table 3, and illustrated in Figures 4-7. Figure 8 shows the performance of RC2-40 versus the base system.

Encryption algorithms and implementations are very complex; minor changes to an algorithm can lead to completely insecure algorithms. Therefore, it is essential that standard algorithms and implementations be used to ensure security. In addition, it is not necessarily the case that algorithms with shorter key lengths lead to better performance. There are many factors affecting performance of an algorithm. Some of these factors are:

- Key setup complexity
- Number of encryption rounds
- Efficiency of the library of encryption primitives that is used
- Complexity of the algorithm

Key length is a factor when determining the time required to "brute-force" all possible keys in an attempt to crack one. For most popular algorithms, however, the trial time for each individual key is normally a function of the algorithm's complexity and not the key length.

DES vs. Triple DES		
Protocol	**Medium file**	**Large file**
IPSec No AH	-28%	-46%
IPSec with AH using MD5	-20%	-38%
IPSec with AH using SHA-1	-23%	-38%
ISAKMP with MD5	-27%	-45%

Table 3. Performance difference between DES and Triple DES. Negative numbers show that the percentage throughput is decreased when Triple DES is used instead of DES.

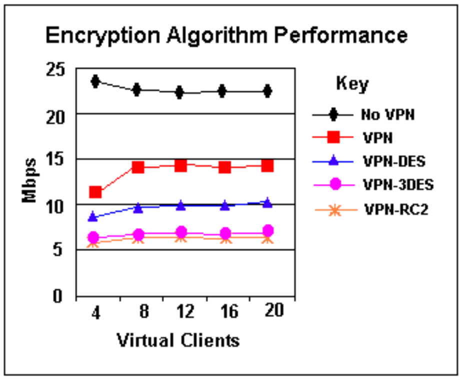

Figure 3. Performance of encryption algorithms (large files)

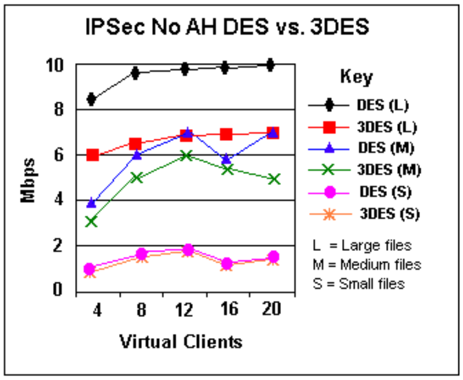

Figure 4. IPSec without authentication headers, DES vs. 3DES

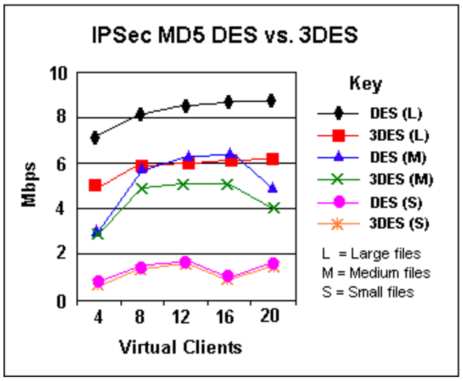

Figure 5. IPSec MD5 DES vs. 3DES

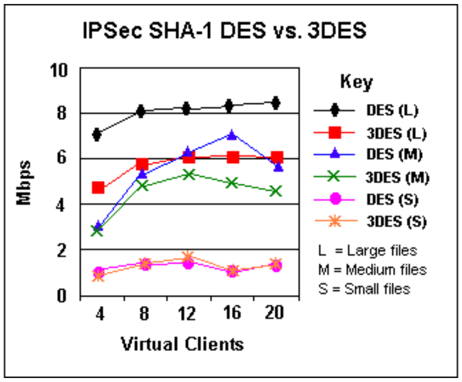

Figure 6. IPSec SHA-1 DES vs. 3DES

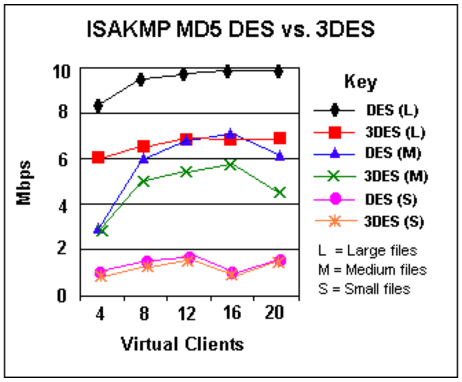

Figure 7. ISAKMP MD5 DES vs. 3DES

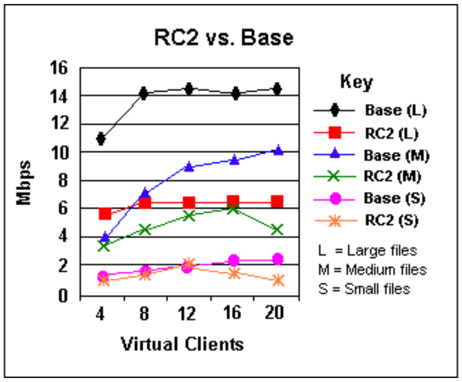

Figure 8. RC2 vs. Base

Authentication

Both the MD5 and SHA-1 one-way hash functions (used for authentication) implemented by the Raptor Firewall were tested. No encryption was done during these tests. SHA-1 is slightly slower than MD5. Throughput degradation was 19% for large files and 22% for medium files for MD5. SHA-1 showed 21% degradation for large files and 18% for medium files. These degradations are shown in Figures 9 and 10. Comparisons were also made between MD5 and SHA-1 for IPSec without encryption and with DES and Triple DES encryption. See Table 4.

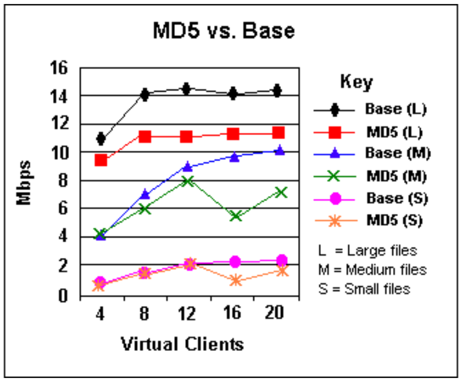

Figure 9. MD5 vs. Base

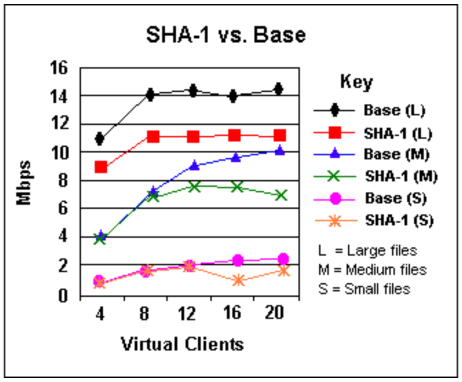

Figure 10. SHA-1 vs. Base

Authentication Headers: SHA-1 vs. MD5		
	Medium files	Large files
IPSec -- no encryption	.04%	-.03
IPSec -- DES	.02%	-.01%
IPSec -- 3DES	-.01%	-.01%

Table 4. SHA-1 vs. MD5. Note: Numbers are SHA-1 relative to MD5. Negative numbers mean SHA-1 is x% slower than MD5, while positive numbers show it is faster

Processor Speed Impact

To test the effect of processor speed on encryption, the original Compaq ProSignia 200 Firewall Servers (266 MHz) were replaced with Compaq ProLiant 1600 Firewall Servers (400 MHz) and Compaq ProLiant 1850R Firewall Servers (400 MHz). Results were nearly identical for the two new machines. Processors improved IPSec processing more than ISAKMP, yet all encryption showed significant improvement. Summary data is shown in Table 5 and individual results in Figures 11-15.

ProSignia 200/266 vs. ProLiant 1850R/400		
	Medium files	**Large files**
swIPe (none)	12%	31%
IPSec (MD5, DES)	29%	36%
IPSec (MD5, 3DES)	23%	39%
ISAKMP (MD5, DES)	22%	27%
ISAKMP (MD5, 3DES)	26%	31%

Table 5. Processor speed impact. Numbers indicate the percentage gain in speed of encryption with a faster processor.

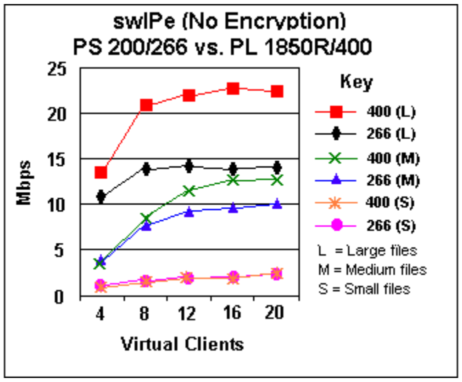

Figure 11. Processor effect on swIPe (no encryption)

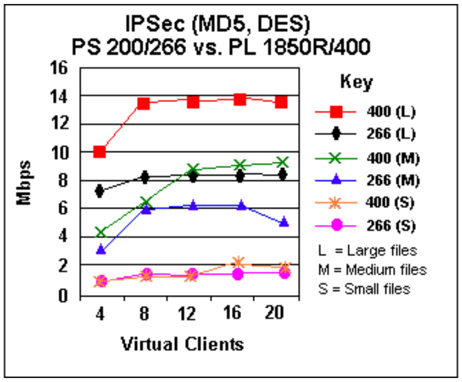

Figure 12. Processor effect on IPSec/MD5, DES

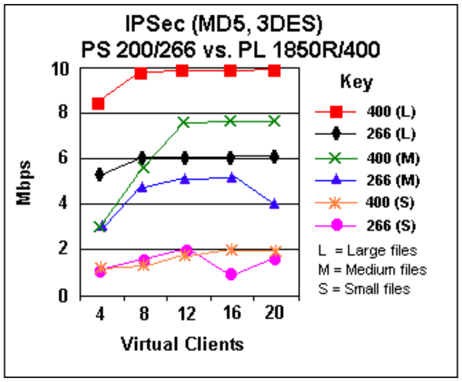

Figure 13. Processor effect on IPSec/MD5, 3DES

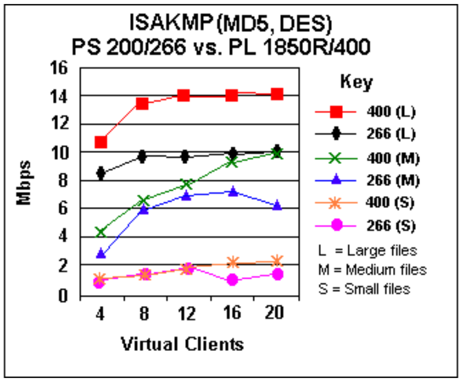

Figure 14. Processor effect on ISAKMP/MD5, DES

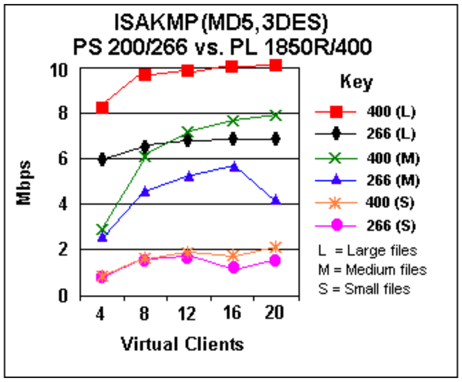

Figure 15. Processor effect on ISAKMP/MD5, 3DES

Replay Protection

Replay protection had no effect on performance.

Transport Mode

Transport mode could not be tested using the methodology described here because transport mode requires the VPN tunnel endpoints to be on the same subnet. This requirement meant that the test client had to be on Firewall Subnet 1, and the Web server on Firewall Subnet 2 (see Figure 1). Under this configuration, the Raptor Firewall required an FTP login (for secure FTP), which the NSTL software does not support.

Conclusion

Introducing VPN tunnels using the AXENT Raptor Firewall 5.0 for NT without authentication and encryption will decrease throughput between two subnets by up to 40% for large files. Compared to tunneling without authentication and encryption, the DES algorithm reduces throughput approximately 30%, Triple DES 52%, and RC2 55% for large files, and a smaller percentage for medium and small files. This performance degradation is very closely tied to file size: the larger a file, the longer it takes to process when encrypting and tunneling over a VPN. For small files, their processing overhead was more significant than the processing overhead created by the encryption algorithm or authentication method used.

The ISAKMP protocol, which dynamically creates IPSec tunnels for ease of administration, is 14% faster for DES using large files, and 7% faster with medium files, than IPSec in a manual mode. The ISAKMP protocol is less processor bound than IPSec. A 400-MHz processor will increase throughput over a VPN anywhere from 20-40% over a 266-MHz processor. Using MD5 authentication is comparable in throughput to using SHA-1, while replay protection can be implemented without any further performance degradation.

A typical VPN installation that provides reasonable security implements IPSec with MD5 and DES. This will result in a throughput of roughly 6 Mbps (for medium-sized files), a 40% reduction over a connection with no tunnel and no encryption. This is equivalent to over three T1 lines, which is sufficient for 90% of today’s Internet connections.