

VPNs: Performance, Security and Management for All

January 2000

By Tadesse Giorgis, Ed Azemar, Farhad Yavari-Issalou, and Linda Victorek

Executive Summary

With the rise of Intranets and Extranets, and a growing number of remote users, net managers who traditionally barred all outsiders from their networks are being increasingly forced to let some in. To accomplish this task today's net managers are taking advantage of Virtual Private Networks (VPNs). These high tech devices enable network administrators to take advantage of a variety of authentication and encryption features that allow for the strictest security over the most public of networks (the Internet) while saving on the cost of leased lines.

In order to evaluate the variety of products that are covered in this report, we divided the products into two major categories. Products designed and targeted for the small to medium business market and those designed and targeted for the large enterprise market. The eight vendors we reviewed represent an excellent cross section of the VPN industry. Their products demonstrate the major approaches to VPN design and implementation that are currently taking place in the rapidly growing Information Technologies (IT) environment. They exemplify the range and quality of VPN products that are available today. For purposes of this review we grouped Compatible Systems Corporation, Intel Networking Hardware Division, Internet Dynamics, and Red Creek Communications in the small to medium business market category. The remaining vendors, Lucent Technologies, Inc., RADGuard, VPNet Technologies, and Xedia Corporation were grouped in the large enterprise market category.

We used NSTL's newly revised VPN methodology to test each VPN product. It is designed to assess VPN security, management, and performance. Security was tested using Internet Scanner 5.8.1 to probe the product under test for vulnerabilities. VPN management was tested using scenario based test scripts that are designed to evaluate remote access, key management, device management, and remote management tools. Performance was tested by measuring the packet-forwarding rate between two VPN gateways, and VPN gateway scalability measured through maximum concurrent connections supported by a VPN gateway.

See Appendix C for further details regarding NSTL's VPN methodology.

Our test results reveal the following two product category winners. In our large enterprise market category Xedia's Access Point™ 1000 had no match in terms of its all-around performance, both in terms of the packet forwarding rate test, as well as their results in our concurrent connection test. In our small to medium business market category Internet Dynamics' IntraPort 2+ posted the highest concurrent FTP connection test-result and achieved the highest overall score in its category. It exhibited excellent performance and showed little performance degradation in our encrypted traffic performance test. Three of the vendors receive NSTL's special honorable mention. The Lucent VPN Gateway (formally Lucent's Brick) had the distinction of withstanding the ISS Internet scanner probe without showing any signs of even potential vulnerabilities. Radguard's cIPro was easy to install and operate, and we noted that it required no in-depth security knowledge, or unique networking skills. Internet Dynamics' Conclave Dynamic VPN was

found to have a wealth of internetworking and security features, and we remind the readers that it would be unreasonable to expect superior performance from a software solution.

Industry Background

The basis for much of the VPN industry's ability to provide a secure method of communication over public networks is contained in the Internet Protocol Security (IPSec) standard that is quickly becoming the basis of interoperable network encryption. This technology was born when the US automotive industry embraced IPSec for use in building an infrastructure for the Automotive Network eXchange (ANX) program. IPSec has continued to gain ground among VPN vendors. Though a basis for an interoperability standard, IPSec still has not reached its full potential. VPN vendors are currently working hard to make true interoperability a feature of their new product offerings.

The Internet was not designed to be a secure and integrated public medium, or to securely transmit important corporate data. A VPN device is designed to offset some of the security concerns of the Internet. Security is the first priority for evaluating any VPN device. But, there is also vital importance in management and performance issues. If a VPN device is difficult to manage its security can be compromised due to human error, and if it degrades performance in encryption mode it can adversely affect the transmission of vital corporate data. The basic principle of secure data transmission over a VPN is that it will scramble information in such a manner that it cannot be understood by anyone except the intended recipient of the information. Moreover, data transmission is intended to be tamperproof. If data is modified during transmission it can be detected and therefore forgery can be prevented. An additional element in the proper functioning of a VPN is its ability to verify the identity of the sender, commonly referred to as authentication. Authentication therefore is an important aspect of VPN's management procedure.

Although, there are pressing security issues and cost reasons encouraging corporations to migrate from the private networks to the VPNs, three challenges persist for those who implement VPNs, they are data security, management, and performance.

It is vital that a network is capable of ensuring authenticity, integrity and the privacy of data. There are, however common security attacks that take place within the wide area network (WAN). The three most frequent instances are denial of service, data tampering, and sniffing. In denial of service hackers clog the system with large amounts of traffic, and crash, or slow down the network. In data tampering, they intercept the packets in transmission and alter contents allowing the packets to reach their destination. This is likely to go unnoticed by the sender or the receiver. In data sniffing, packets are intercepted within the WAN preventing them from reaching the intended receiver, or at other times packets are allowed to reach their destination with receiver and the sender remaining unaware that there was any kind of interception. With these types of threats within the WAN and many more like them, it is likely that creating a VPN will work towards keeping data private, and being able to account for the authenticity of the received information.

In management, remote configuring and monitoring of the device are significant areas of concern and there are two essentials: key management and device management. How quickly could a net manager remotely (e.g., from his home in the middle of the night) revoke a compromised key; verify that VPN device drops all active sessions; and disable the VPN device's external interface? Or, what would be entailed in the changing of rules: Do rule changes require a reboot? Are the remote commands sent in encrypted form to safeguard the configuration sessions? Or does

enabling new rules cause active sessions to be dropped? These are some of the challenges confronting VPNs as security devices used to safeguard information travelling across the WAN.

While security is the very reason why VPNs exist, yet, at the same time, it would be unrealistic to expect that end-users can tolerate any cost that this would exact on performance. Naturally, end-users care about response time and not much about throughput. But these performance measurement metrics are not necessarily independent from each other. If authentication and encryption overhead is noticeably higher than the performance of data traffic in the clear, then this becomes unacceptable. That is why VPN vendors are implementing encryption in their hardware appliances and this has enabled them to partially achieve their objective, although there is still some room for improvement. The other performance issue is scalability, measured in terms of the number of simultaneous tunnels that a VPN gateway can sustain without degrading response time and other performance characteristics. For large enterprise or ISP implementations, not only is the number of simultaneous client-to-gateway tunnels important, but also gateway-to-gateway connections, for dense meshed configuration support.

Technology Background

How VPNs work

The idea behind VPN devices is to use the more economical Internet rather than leased lines. VPNs are placed between private and public domains in networks to enforce dedicated secure paths, or tunnels. VPNs then encrypt corporate network data before it gets to hostile environment of the Internet and decrypt it before data is to be viewed at the permitted workstations. VPNs ease the transmission of data to the dial-up access points by protecting the information against interception and intrusion over public networks.

Tunneling, the process of encapsulating and transmitting data packets of one specific (client) transmission protocol over that of another (host) protocol is the underlying scheme behind VPN technology. A tunneling protocol simply wraps the data and header information of the client transmission protocol in a new header of the host protocol to provide routing information, so that the encapsulated payload can reach its final destination. A VPN tunnel not only wraps a payload in a new header so that it reaches its final destination, but it also makes sure that it reaches its final destination securely and without tampering, while using the public network. Transmission of data over the Internet, or other public networks via a VPN tunnel makes use of several different types of tunneling techniques, such as PPTP (point-to-point tunneling protocol), L2FP (Layer 2 forwarding protocol), L2TP (Layer 2 tunneling protocol). IPSec is a Layer 3 protocol that adds data authentication and encryption to a VPN tunnel to ensure security.

Key IPSec Components

Note: A complete technology summary is available in the full version of this report.

It is important to remember that IPSec is currently only a series of guidelines for the protection of Internet Protocol (IP) communications. Its specification details various ways for securing private information transmitted over public networks. Various services supported by IPSec include confidentiality (encryption), authenticity (proof of sender), integrity (detection of data tampering) and replay protection (defense against unauthorized re-sending of data). IPSec also contains methodologies for key management. Internet Key Exchange (IKE), the IPSec key management

protocol, is a series of steps that authorize keys for encrypting and decrypting information. It defines a common language on which communication between two parties is based. IPSec methods of secure transmission of data have specific standards. IPSec has a two pronged approach and uses ESP (encapsulating security payload) and AH (authentication header). ESP sets in process the encrypting an entire packet and placing it inside a larger packet. This method of tunneling is secured further with the AH, which finds a way to authenticate the traffic but not encrypt it. Using this two pronged method security for network traffic is enhanced.

See Appendix B for details regarding relevant RFC documents.

Recent Trends and Challenges

Note: A complete summary of recent trends and challenges is available in the full version of this report.

Vendor Summaries

Large Enterprise Market VPNs

Xedia AccessPoint 1000

The Access Point™ 1000 is a high-end Internet access router designed to provide multiple IP services including secure IPSec tunneling. It can be deployed as part of a carrier managed service, such as one provided by an ISP, or as part of an enterprise network infrastructure of a large corporation. With its tight security features, performance, and scalability, the Access Point 1000 is ideally suited to operate as a fully integrated VPN router or a QoS-enabled VPN gateway in large traffic centers. According to the vendor's information, the system supports secure site-to-site and remote access VPNs with up to 4000 IPSec tunnels. We found that Xedia's AccessPoint VPN gateway had no match in terms of its all-around performance showings, both in terms of the packet forwarding rate test, as well as the concurrent connection test. While the VPNet VSU-1100 showed a better result in the concurrent connection test, it must be noted that this was not an apples-to-apples comparison test. The Xedia gateway was configured to handle 500 simultaneous tunnels with 500 corresponding SAs, while the VPNet VSU-1100 could only be tested in a single-tunnel configuration with only one SA. Xedia's AccessPoint VPN placed first in the overall evaluation among VPN gateways in the large enterprise market product category.

The Access Point 1000 does IPSec tunneling and encryption. It is a L2TP (tunneling protocol) Network server. It is integrated with a packet filtering firewall and it supports up to 4000 IPSec tunnels both site-to-site and remote access. It also supports triple DES. The IPSec tunneling and encryption supports both 56-bit DES and 168-bit DES encryption, with HMAC-MD5 and HMAC-SHA1 message authentication. The user level authentication is supported with Remote Authentication Dial-In User Service (RADIUS) and local passwords. The system also supports X.509v3 formatted digital certifications.



Xedia Corporation is located in Acton, MA. They can be contacted at (978) 263-0060 / www.xedia.com. In November 1999 they were acquired by Lucent Technologies. Their product, the Access Point 1000 is hardware based and uses a MIPS R7000 @ 262 MHz processor. The product as configured for this test sells for \$19,995, plus the QVPN software, which has a list price of \$1,000. Management applications, including QVPN Builder are available at no charge. The product supports firewall router functionality, IP router functionality, and bridging mode.

Lucent VPN Gateway

By design, the Lucent VPN Gateway is optimized for maximum security. This security feature usually comes with some sacrifice in performance, and it is reflected in the performance numbers of the Lucent VPN Gateway product. Unlike other VPN gateways tested, where the hardware and software are housed in the same box, the hardware (the VPN appliance) and software (the VPN Gateway Management Server) are separate components in the Lucent VPN product. The Lucent VPN Gateway functions as an IPSec tunnel endpoint to set up encrypted communication pathways between itself and another IPSec compliant device. It can be configured to support multiple zones on each interface with each security zone having its own secure IPSec tunnel. It can support both LAN-to-LAN and Client-to-LAN configurations. The Lucent VPN Gateway Management Server is designed to configure, administer and update multiple bricks, security zones, and VPNs from a single workstation. It performs all VPN policy decisions such as IKE key management and SA negotiations. Although its performance in our encrypted traffic packet forwarding rate test was not spectacular, the Lucent VPN Gateway posts very respectable performance results in both the packet forwarding rate test and the concurrent connection test.

Lucent's VPN Gateway is an integrated firewall/VPN hardware appliance that includes router functionality. The high scalability of the product makes it possible to manage hundreds of firewall/VPN gateways and many more IP Sec client users using one console. The system administrator controls all the configuration information. The information is automatically downloaded to the IP Sec client over a secure channel. It supports Triple DES and RC4 128-bit range and provides integrated and external CA. The product successfully withstood the ISS Internet scanner probe and was the only product tested that did not show some potential vulnerability.



Lucent Technologies is located in Murray Hill, NJ. They can be contacted at (732) 615-2759 / www.lucent.com. Their product, Lucent VPN Gateway is hardware based and uses a 333 MHz Intel processor. The product as configured for this test sells for \$21,990 and includes two Lucent VPN Gateway appliances, Lucent Security Management Server Software, Lucent IPSec Client software and a license for 100 simultaneous VPN sessions. It supports firewall router functionality, IP router functionality, and bridging mode.

VPNNet VSU-1100

The VSU-1100 is a high-end VPN gateway for secure business communications applications. It can be used by large enterprises building their own VPNs, by network service providers deploying managed VPN services, and by application service providers (ASPs) delivering business-critical solutions to enterprise customers. The VSU-1100 supports a full suite of VPN services such as ICSA-certified IPSec-based encryption; packet compression and authentication; user authentication; IKE and SKIP key management; Network Address Translation (NAT); and digital certificates. For encrypted traffic, VPNNet's VSU 1100 achieved the second best performance for all packet sizes. It also posted a high test score of 102,000 simultaneous FTP connections.

The VSU-1010 supports DES encryption with 56-bit key and Triple DES encryption with 168-bit key. The product is also capable to discard weak and semi-weak keys. It does packet authentication keyed MD5, AH Message Digest Algorithm (RFC 1321) and it also does HMAC-MD5 and HMAC SHA-1 (RFC2104). It will authenticate the users using RADIUS servers, CHAP and PAP, and SecureID tokens. It is able to inspect the source address of all packets being sent to the tunnel between the client and the network. During our security tests we were able to compromise the tunnel between the client machine and the network. VPNNet has told us that they have since investigated the "source address inspection" and have gone on to build additional security protections in the pending release of their VPN remote client.

VPNNet has indicated that they will introduce a new GUI in the fourth quarter. Their current Java based software, which is slow, will be replaced with a more standard Windows based interface. VPNware™ offers scalability to support large-scale enterprise networks. Using Dyna-Policy Download™ the user is able to automatically update remote clients with the latest policy information. Client users automatically receive updated policy information when they access the VPN. The System Management includes, configuration using the Java-based VPNmanager™, configuration traffic that is secured through SSL, secure software downloads for system upgrades and Syslog event and usage logging. Remote Client Support includes, VPNremote Client

Software for Windows 95/98 and Windows NT. VPNet's VPNware Tool Suite allows the user to manage virtual private networks with a Web browser.



VPNet Technologies, Inc. is located in San Jose, CA. They can be contacted at (408) 445-6600 / www.vpnet.com. Their product, the VSU-1010 hardware based. The product as configured for this test sells for \$4,995 for one site, \$9,990 for two sites, and the VPNmanager MultiSite sells for \$1,995. A single client license sells for \$99. It supports firewall router functionality, IP router functionality, and bridging mode.

RadGuard cIPro-VPN

Radguard's cIPro-VPN is a highly secure, hardware-based VPN gateway that can be used in Intranets, Extranets, multi-party VPNs, and secured virtual private links to mobile users. The cIPro-VPN employs hardware-based certificate authority and is compatible with the IPsec and X.509 standards. It is extremely easy to install and operate and requires no in-depth security knowledge or unique networking skills. An easy to use GUI management package, running under HP Open View®, provides effective management of all TCP/IP network VPN devices. The cIPro's performance results were somewhat limited due to incompatibility problems with the Cisco Catalyst 2926 FastEthernet switch that was used in our test bed. Although the nature of this problem was not fully understood at the time of our test, the product's performance in a shared (10/100 hub) network environment was much higher. The test results contained in this report were obtained using the Cisco switch.

The product complies with IPsec, ISAKMP/Oakley. Its encryption and key management is implemented by hardware. It has integrated firewall and NAT functionality, and it provides a rapid and random key generation system. It also provides automatic topology learning and adaptation. The cIPro client is IP sec compliant and it uses the standard Microsoft stack. It operates transparently to the user and it supports any networking media. When subjected to our tunnel compromise test, the cIPro client was the only device that did not allow browsing of the network neighborhood while the drives were shared. We found the cIPro VPN system to have solid and well-featured security functions both at the gateway and client locations.





Radguard is located in Tel Aviv, Israel. They can be contacted at (201) 828-9611/
www.radguard.com. Their product, the cIPro System is hardware based and uses an Intel I960H processor. The product as configured for this test sells for \$14,950 and includes two VPN devices with firewall capabilities, and CA and management software. It supports firewall router functionality, IP router functionality (static routing only), and bridging mode.

Small to Medium Business Market VPNs

Compatible Systems IntraPort2+

The IntraPort 2+ is designed for medium-sized businesses, or large branch offices, that need up to 500 simultaneous remote access sessions and/or up to 32 site-to-site connections. The IntraPort 2+ supports DES and 3DES encryption with a built-in hardware co-processor. In the packet-forwarding test among the small to medium business market VPN products, the Compatible Systems' IntraPort2+ exhibited very good performance, showing little performance degradation in encrypted traffic performance. It also posted the highest concurrent FTP connection test-result in the small to medium business market group. Compatible Systems' IntraPort2+ achieved the highest overall score in NSTL's the small to medium business VPN category.

Typically the company using the Intraport 2+ will have, or is planning to have, multiple T1s. Compatible Systems offers several other Intraport product family members that appeal to other market segments. Their Intraport 2 is their low end product and it does not have an encryption card. The unit's processor does all the encryption. This product is targeted for sites with Internet connections of T1 or less.

Compatible systems' IntraPort2+ provides IP Sec, DES and Triple DES support (both in gateway and client). In RC4 bit range it also supports PPTP. Its encryption is hardware based, which further shields the gateway from break-ins. It is able to tunnel multiple protocols. It uses MD5 or SHA digital signatures to authenticate each packet of data in IPsec tunnels. Remote clients have the option to use either RADIUS, or secureID servers.



Compatible Systems Corp. is located in Boulder, CO. They can be contacted at (303) 444-9532 / www.compatible.com. Their product, the Intraport 2+ is hardware based and uses a StrongARM RISC @166Mhz processor. The product as configured for this test sells for \$10,000 per unit, management application is free, and there is no charge for software updates for the life of the product. It supports IP router functionality and bridging mode.

RedCreek Communications Ravlin 7100

RedCreek's Ravlin 7100 secure VPN solution is targeted towards intermediate to larger size corporations that require Fast Ethernet speed and support for site-to-site and remote access connections. Network administrators may also deploy the Ravlin 7100 to establish private communications within secure Intranets (between corporate divisions, workgroups, and branch

offices) or within secure Extranets (between customers, suppliers, and strategic partners.) In the packet-forwarding rate test, the Ravlin product showed very good performance in the clear-text traffic for all packet sizes (25/50/98 Mbit/sec for 64-/256-/1406-byte), although that good performance did not readily extend to the encrypted traffic test. It also showed the second-best performance in the concurrent connection test among intermediate VPN products.

The Ravlin 7100 is a software application independent gateway that fully implements IP security standard (IPSec). It uses 56-bit Data Encryption Standard (DES) and 168-bit Triple DES encryption, and provides access control and authentication using DSS (Digital Signature Standard), Diffie-Hellman key exchange, X509 v.3 digital certificates, and IKE key management. The product can operate in different modes for meeting different security needs. In the ESP (Encapsulating Security Payload) Tunnel Mode the device provides its highest level of security between gateways. In the ESP Transport Mode, it encrypts only the payload of the original IP datagram. In the Encrypt-In-Place (EIP) Mode, the product only encrypts the payloads of IP datagrams. These capabilities amount to strong security enforcement features.



RedCreek Communications Inc. is located in Newark, CA. They can be contacted at (510) 745-3900/ www.redcreek.com. Their product, the Ravlin 7100 is hardware based and uses an Intel i960 processor. The product as configured for this test sells for \$7,500 per system, \$1,000 per Ravlin Node Manager and \$99 per Ravlin Soft Client. It supports limited firewall router functionality and bridging mode.

Intel LanRover VPN Gateway

The LanRover VPN Gateway is a VPN tunnel server and comes with full authentication, data encryption, routing capability, and firewall functionality, and the product is scalable. These features give it a strong security base. Moreover, the tested model has a crypto accelerator card using ASICs (application –specific integrated circuit) that accelerate standard and triple-DES encryption. The product supports DES and Triple DES both with the gateway and client. It supports integrated CA and external CA on both the client and gateway. Moreover, it has token authentication cards on both the client and the gateway systems, which further facilitates security measures.

Intel's target markets includes network managers at small and medium enterprises and ISPs with anywhere from 25 to 2,500 employees. Intel's LanRover VPN Gateway is a dedicated, hardware-based and IPsec-certified solution, and it includes a built-in firewall and can support up to 1024 simultaneous tunnels. The LanRover VPN Gateway's performance evaluation scores are only better than that of the Internet Dynamics Conclave Dynamic VPN that is a software solution. If Intel has plans to maintain the LanRover product family, it has a lot of work ahead of it for the next release of the software to upscale the product's performance.



Intel Networking Systems is located in Bedford, Mass. They can be contacted at (781) 687-1000 / www.intel.com. Their product, the LanRover VPN Gateway + is hardware based. The product as configured for this test sells for \$9250 per unit. Their management application sells for \$1250 (for 1000 users). It supports firewall router functionality, IP router functionality, and bridging mode.

Internet Dynamics

The Internet Dynamics Conclave product family is an integrated set of software solutions built around a common role-based policy management environment. Conclave features an incremental deployment approach that allows small initial installations to easily grow into any of the more complete enterprise solutions including scalability that would allow expansion in number of sites, users, servers, applications, or functionality. The Conclave Dynamic VPN solution is a member of this suite of products and is designed to offer secure access to resources between several Intranet sites, or between remote sites over the Internet. The same VPN solution can also be used to implement Extranets with business partners. As might be expected from a software-only VPN solution, the performance of the Conclave Dynamic VPN was relatively poor compared to the other vendors participating in our test. However, it would be unreasonable to expect superior performance from a software solution with a wealth of internetworking and security features, especially when it is stacked against dedicated hardware-based VPN solutions.

Using Conclave access control allows the user to access the information that they want to share and only that information. Employees can even use Microsoft file sharing just like they do on their own local network. Conclave provides five ways of identifying employees. If running a Microsoft NT Domain you can leverage your already existing NT security database. Conclave will identify and authenticate your employees using their Windows ID. You can use the integrated Conclave Certificate Authority to issue X.509 certificates to employees. These certificates can be used for identification and authentication as well. In addition Conclave can also use certificates issued by other Certificate Authorities. For companies that use tokens such as SecurID cards, Conclave can use them for identification and authentication. Finally, Conclave can use standard IP addresses and IP domains to identify employees.



Internet Dynamics, Inc. is located in Westlake Village, California. They can be contacted at (805) 370-2200 / www.conclave.com. The product as configured for this test sells for \$5400, plus \$20 per client.

Testing Analysis

Market Basics

We set out to explore the security claims made by the participating VPN vendors and to find out just what network managers can expect when implementing a VPN solution. Using NSTL's latest VPN methodology, eight products were put through common configuration and administration scenarios, to determine the performance penalties that such administration and management policies exact. What was our basic finding? There are big differences among the current crop of VPN products, not only in how they are constructed but also in their performance.

There are three main areas involved in NSTL's VPN methodology: security, management, and performance. We test VPN security using Internet Scanner 5.8.1 to probe the product under test for vulnerabilities. The software is run from the unprotected side of the gateway. We test VPN management using scenario based test scripts. These are designed to assess remote access, key management, device management, and remote management tools. Our VPN performance test is made up of two components: packet-forwarding rate between two VPN gateways and VPN gateway scalability measured through maximum concurrent connections supported by a VPN gateway.

See Appendix C for further details regarding NSTL's VPN Methodology.

In most of its reviews NSTL evaluates products and systems that are pretty much similar to one another, but not so this time. In order to evaluate the range of VPN products included in this review, we divided the products into two major categories. VPN products produced for the small to medium size business market and those produced for the large enterprise market. We defined VPN products fitting into the small to medium business market as those products supporting small and medium enterprises and ISPs. Intel's LanRover VPN Gateway is an example of a small to medium business market product. We defined the large enterprise market as those products supporting large distributed enterprise networks and Internet Service Providers (ISPs). Lucent's VPN Gateway, a dedicated high performance VPN appliance offering managed VPN/firewall services, is an example of a large enterprise market product.

In addition, one of the VPN products was software based (Internet Dynamics) while others were a combination of hardware and software. Most included routing and firewall (access control) functions (e.g., Lucent Technologies), while a few focused solely on authentication and encryption. We found the VPN vendors in this review supporting a wide variety of authentication methods, including token authentication cards, Radius servers, and a wide variety of encryption algorithms.

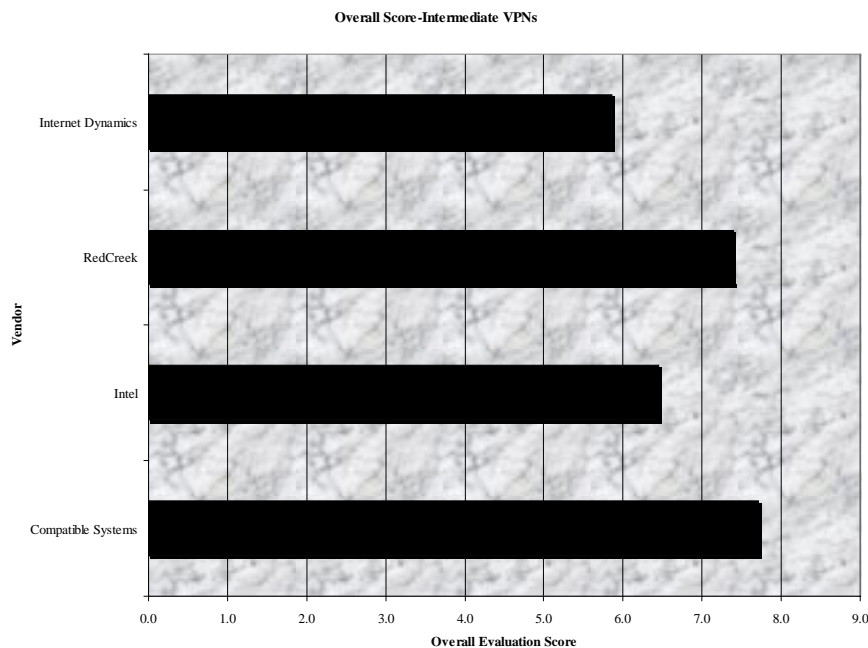
Another way to distinguish between various approaches to VPN technology is whether a product has router and firewall functions. Strictly speaking, firewalls handle access control and VPNs handle authentication and encryption. Since these are complementary functions, they can be implemented in the same product, but they don't have to be, and there's no one right answer as to whether they should be. Companies that buy all their security products from one vendor deal with fewer platforms, and that means fewer management hassles. On the other hand, there's a school of thought that says putting multiple security functions on one platform is risky because it makes for a single point of failure. Further, vendors of standalone devices generally offer more sophisticated VPN features and in some cases higher performance due to their ability to move their programs from slower software to the latest high speed Application Specific Integrated Circuits (ASIC) technology.

Overall Evaluation

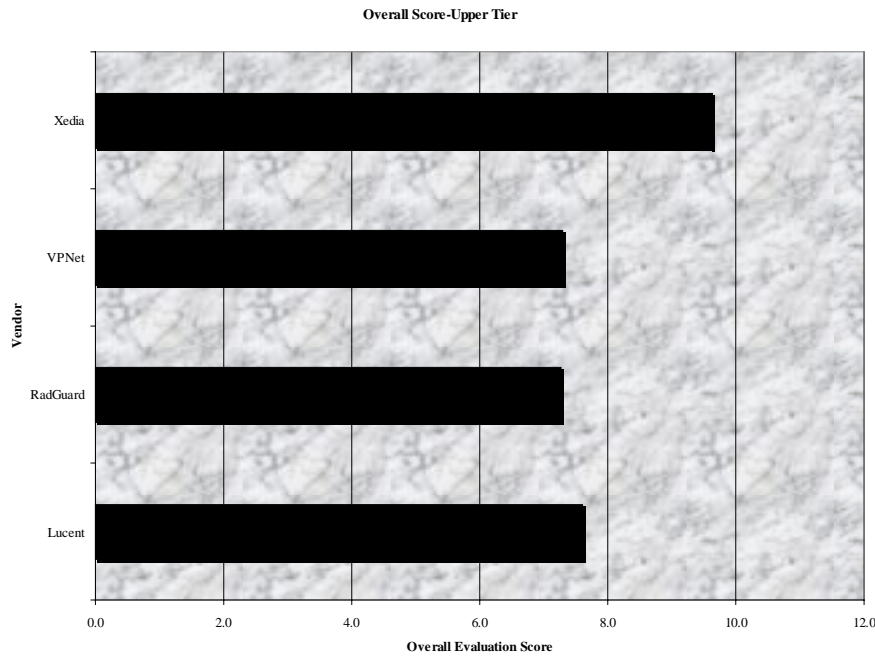
NSTL's overall test results for the 1999 VPN gateway evaluation consists of three components: VPN gateway security evaluation, VPN gateway administration and management evaluation, and VPN gateway performance evaluation. The overall evaluation score is a weighted-average of these three categories.

$$\text{Overall Evaluation Score} = 40\% \times (\text{Security Score}) + 25\% \times (\text{Management Score}) + 35\% \times (\text{Performance Score})$$

Among the small to medium business VPN products, Compatible Systems' IntraPort2+ achieved the highest overall score, with RedCreek's Ravlin 7100 close behind. Although both the IntraPort2+ and the Ravlin 7100 earned an identical score in the security evaluation, the Ravlin unit displayed a better management score while the IntraPort2+ received a higher performance score.



Xedia's AccessPoint VPN far outscored its competition in the overall evaluation among VPN gateways in the large enterprise market product category. It received by far the best performance and management scores and finished a close second in the security evaluation behind the Lucent Technologies' VPN Gateway. Excellent encryption performance coupled with a near-perfect management score helped the Xedia product achieve such a solid standing.



Security Evaluation

The security features of this current crop of VPNs have definitely been strengthened compared to what was seen in past NSTL reviews. In September 1997, NSTL did its first major evaluation of VPNs, and most of the products did only encryption and authentication (see "VPNs: Security With an Uncommon Touch," - Data Communications Magazine). In July 1998, five devices out of a total of six had routing capabilities and three functioned as firewalls (see "VPNs: Safety First, but What About Speed?" - Data Communications Magazine). We found this year that the eight products that were reviewed functioned as routers and served as firewalls. These common areas of improvement complemented IETF's (Internet Engineering Task Force) set of TCP/IP security specifications. All the products that we tested were IPSec compliant, however the concept of compliance can be misleading, and definitely does not mean interoperability at this stage of VPN development. It is important to note that IPSec defines two types of key exchange methods and not all the products comply with the same methods. There is the IKE (Internet Key Exchange, formerly referred to as ISAKMP/Oakley) key exchange method, and there is a method of key exchange called SKIP (Simple Key Exchange Internet Protocol). All VPN vendors comply with IKE but they don't all use the same version of it. In addition, encryption algorithms are not standardized which is partly due to the export restrictions.

Note: A complete description and analysis of the security components used for this review are available in the full version of this report.

The ISS Internet Scanner Test

Note: A complete description and analysis of the security components used for this review are available in the full version of this report.

ISS Internet Scanner Reports

Note: A complete description and analysis of the security components used for this review are available in the full version of this report.

The Tunnel Compromise Test

Note: A complete description and analysis of the security components used for this review are available in the full version of this report.

Tunnel Compromise Test Results

Note: A complete description and analysis of the security components used for this review are available in the full version of this report.

Management Evaluation

The management evaluation consisted of a series of scenario-based tasks that imitate those that are regularly performed by VPN users and network managers. We used these scenario-based tasks to test each product for ease of remote management tasks, remote management tools, device management tasks and key management tasks.

Note: A complete description and analysis of the management evaluation for this review are available in the full version of this report.

For further information regarding NSTL's scenario-based management tasks see NSTL's VPN Methodology in Appendix C.

Performance Evaluation

The VPN gateway performance evaluation is made up of two components: packet-forwarding rate between two VPN gateways and VPN gateway scalability measured through maximum concurrent connections supported by a VPN gateway.

In the first performance test category, we look at the packet forwarding speed of each VPN gateway in two security configurations: data transmitted in the clear (with only message authentication enabled) and data transmitted with message authentication and data encryption (using triple DES) enabled. The objective of this test is to find the maximum throughput that each VPN gateway could sustain at different frame sizes without dropping packets.

In the second performance test, the interesting test result is the number of simultaneous tunnels established and maintained between remote clients and a single or multiple VPN gateways.

However, we found that simulating multiple remote clients without physically installing multiple remote VPN client software on multiple systems is quite a challenge. We attempted to simulate the multiple remote client connection scenarios through the creation of multiple user groups and/or IP subnets behind one VPN gateway. These multiple user groups and/or IP subnets are connected to one or multiple hosts behind the other gateway. In the test configuration, ten subnets (192.168.4.0/24 through 192.168.14.0/24, subnet 192.168.9.0 is skipped) behind the Branch gateway, each with 250 IP addresses, are connected to two servers (192.168.1.226 and 192.168.1.227) at the Headquarters LAN.

Packet Forwarding Test

Note: Full details regarding the test structure used by NSTL are available in the full version of this report.

Concurrent Connection Test

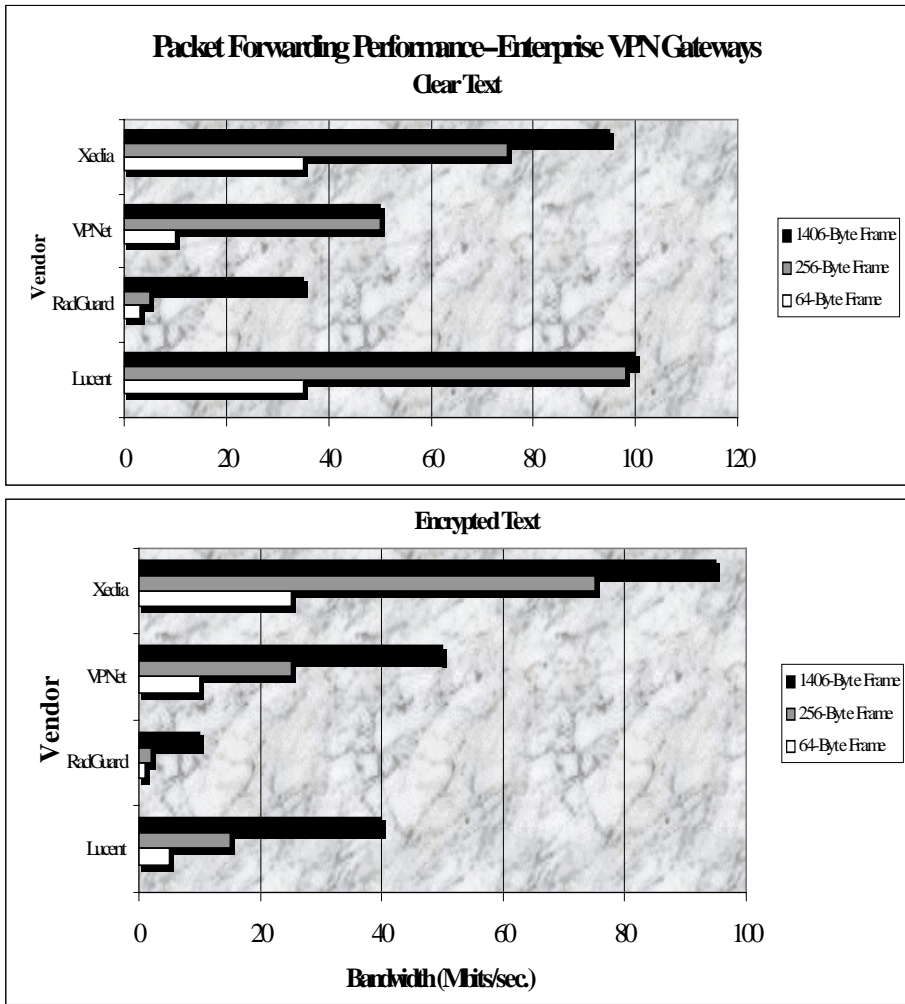
Note: Full details regarding the test structure used by NSTL are available in the full version of this report.

Performance Results and Analysis

The following chart summarizes the packet-forwarding performance of all products in the large enterprise market category for clear and encrypted traffic for all packet sizes.

Note: A complete description and analysis of the performance tests used in this review are available in the full version of this report.

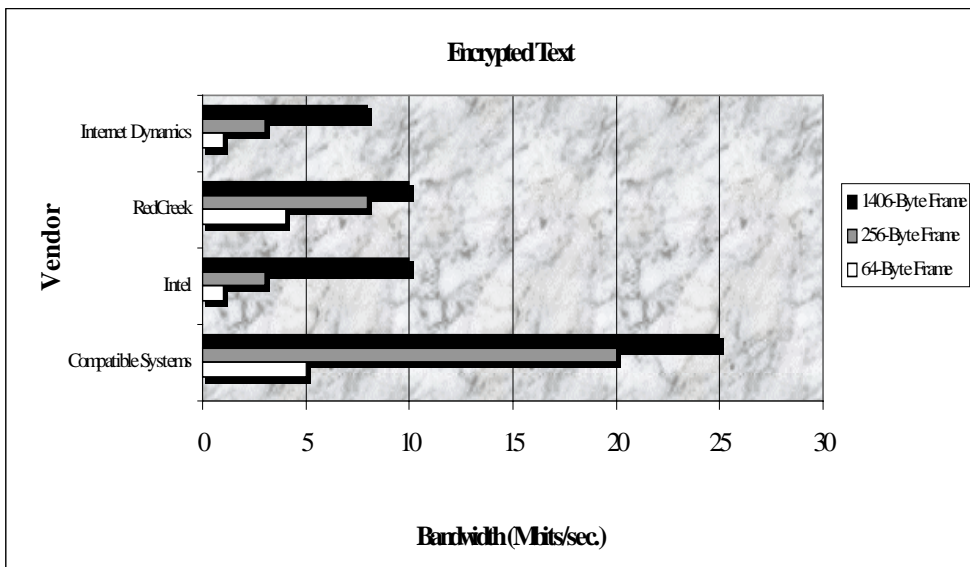
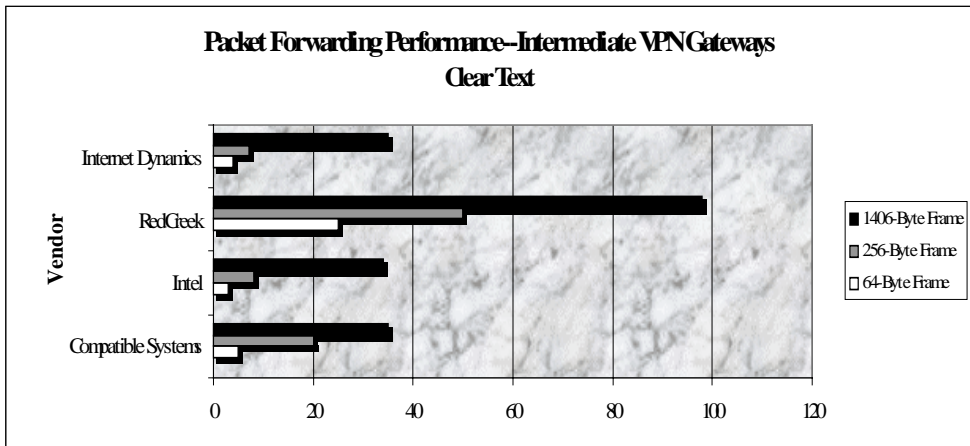
The following chart summarizes the packet-forwarding performance of all products in the large enterprise market category for clear and encrypted traffic for all packet sizes.



The following chart summarizes the packet-forwarding performance of intermediate market VPN products for clear and encrypted traffic for all packet sizes.

Concurrent Connection Test

Note: A complete description and analysis of the performance tests used in this review are available in the full version of this report.



Concurrent Connection Test

Note: A complete description and analysis of the performance tests used in this review are available in the full version of this report.

Conclusion

Top Performers

Small to medium business market

Best overall score went to Compatible Systems' IntraPort2+ followed closely by RedCreek's Ravlin 7100. We salute Compatible Systems for their excellent encryption performance and RedCreek for their near-perfect management score. In our the packet forwarding tests RedCreek obtained the highest score in the clear text packet forwarding test and Compatible Systems obtained the highest score in our encrypted packet test. We like RedCreek's Ravlin Node GUI, and found it

more than adequate for the small to medium business market that the Ravlin 7100 was designed for.

Large enterprise market

Best overall score went to Xedia's AccessPoint VPN followed Lucent Technologies' VPN Gateway. We salute Lucent for their excellent security features. In our the packet forwarding tests Lucent obtained the highest score in the clear text packet forwarding test and Xedia obtained the highest score in our encrypted packet test. In our management test Xedia obtained the highest score followed closely by Radguard. We liked the ease of use and powerful features of Xedia's QVPN Builder VPN policy manager and found it well suited for the large enterprise market for which it was designed.

Honorable Mention

Lucent

Lucent's VPN Gateway receives honorable mention for its security features. Of all the products tested they had the distinction of withstanding the ISS Internet scanner probe without showing any signs of even potential vulnerabilities. Lucent's VPN Gateway is an integrated firewall/VPN hardware appliance that includes router functionality. The high scalability of the product makes it possible to manage hundreds of firewall/VPN gateways and many more IP Sec client users using one console.

Radguard

Radguard's cIPro-VPN receives honorable mention for its management. It is extremely easy to install and operate and requires no in-depth security knowledge or unique networking skills. An easy to use GUI management package, running under HP Open View®, provides effective management of all TCP/IP network VPN devices. Radguard received the second highest management score in the large enterprise market group coming in just behind Xedia's product. Unique to Radguard's client, and reinforcing its already strong security features, is the fact that it does not allow browsing of network while drives are shared.

Internet Dynamics

Internet Dynamics' Conclave Dynamic VPN receives honorable mention. We salute the product's wealth of internetworking and security features and remind the readers that it would be unreasonable to expect superior performance from a software solution. Internet Dynamics has designed their product for the small to medium business market. It is designed for those looking for a dynamic, scalable VPN that can grow as their business grows.

Appendices

Note: Appendices are not available in the freely distributed version of this report.