Lucent Technologies
Bell Labs Innovations



WHITE PAPER

DIY or Outsourced: SecureVPN Strategies for the Enterprise

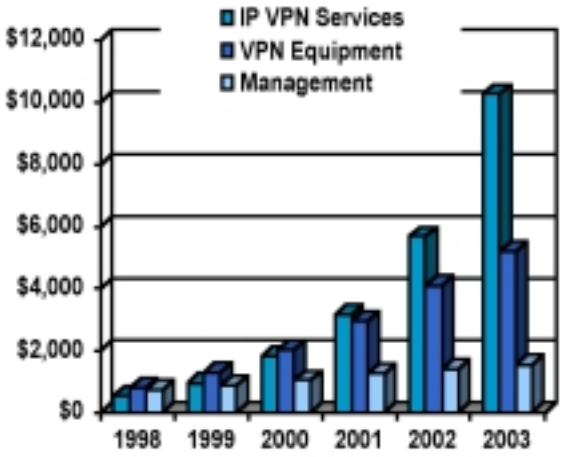
Building Enterprise VPNs With End-to-End Security, Performance, and Customer Control

05-91
2/00

I. VPN Services

eBusiness opportunities are driving enterprise demand for flexible and secure wide-area communications. Deeply entwined with Internet connectivity and IP networking advances, the need for companies to exchange information with customers, suppliers and business partners anywhere, globally is growing beyond the scope of traditional network solutions. As businesses leverage their reach in what is increasingly defined as the "virtual enterprise," IP-based Virtual Private Network (VPN) solutions are proving to be one of the most enabling solutions for achieving global connectivity.

Across the board - from organizations with three networked sites to multinational companies with 50,000 mobile users - enterprises are choosing IP-based VPNs for their wide area networks. According to late 1999 market research by Telechoice, Inc., one-third of the companies that rely on wide area networks are already using VPN services either in production or in trials. Analysts predict that business customers will spend over $14 billion annually on VPN equipment and services by 2003.



Services	**81%**
Equipment	**42%**
Management	**16%**
US/Europe	**37-40%**
CALA/APAC	**45%**

Source: TeleChoice, Inc.

*Figure 1—**Global VPN and Managed Services Growth***

While enterprises acknowledge the critical role that the Internet and IP VPNs will play in their strategic eBusiness initiatives, there are different paths by which a VPN could be implemented. The options range from being fully built, owned and operated by the enterprise to being fully outsourced to a partner. In fact, it is generally believed that enterprise-operated and managed VPN services will hover around a 50/50 split, including hybrid approaches, for the near term.

©2000 Lucent Technologies, Inc.

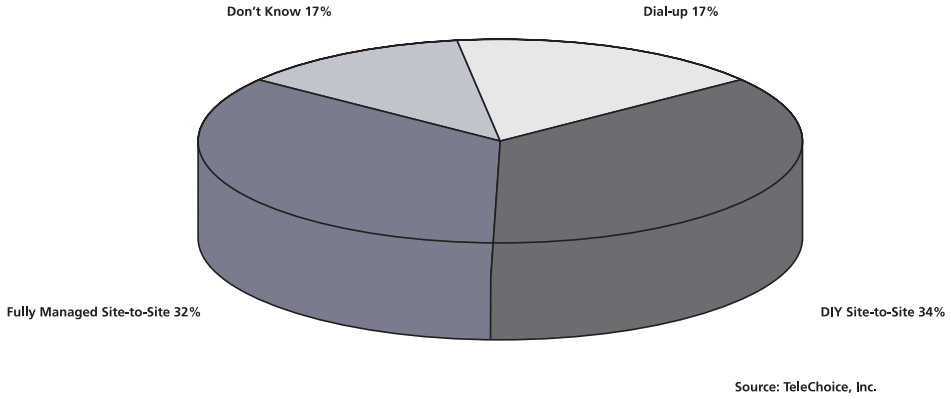


*Figure 2—**VPN applications***

Self-Managed, Outsourced, or Both?

Increasingly, customers are assessing their VPN implementation options across a spectrum of Do it Yourself (DIY), fully outsourced, or hybrid models. Each approach brings a unique business advantage.

- Do it Yourself: Operates over a public network facility (most commonly the Internet), with equipment owned and operated by the enterprise. The greatest benefit is the degree of flexibility and control the enterprise has over VPN deployment, administration and adaptability or change.
- Fully Outsourced: A managed service which could be implemented by a collection of partners including an ISP and a security integrations partner. Advantages include quick deployment, easy global scalability, and freedom from overhead network management.
- Shared Management: A hybrid approach where a partner may take responsibility for major elements of infrastructure deployment and management, but the customer retains control over key aspects of policy definition and security management.

The Do it Yourself Option

Current market research indicates that most VPN implementations today, including dial-up remote access solutions, are owned and operated by the enterprise. While many reserve the option to outsource part or all of their VPN at some point along the way, they are investing in the resources necessary to initially trial and then scale to a broader set of applications on their own.

The reasons most often include a business-centered need to retain control of either key policies or administrative tasks. For example:

- Some enterprise organizations must retain sole control over all elements of their network security as part of their corporate charter.
- Other enterprises may rely on their network as a strategic element of their business. In this environment they may need the ability to rapidly adapt to unique customer or business needs, requiring the immediate response and degree of control that comes with fully retaining network operations within the business.

©2000 Lucent Technologies, Inc.

In some cases a customer may start with a DIY strategy and then migrate to a managed service. In fact many are asking their equipment vendors to bring an ISP and a security expert to the table to better assess how their VPN solution might migrate over time. Once the core VPN is in place with the appropriate definition and policies, the best way to scale the VPN may in fact be with a global managed services partner. In fact the recent Telechoice research found that outsourcing is the number one change that today's DIY enterprise VPN manager have planned.

The reason is straight-forward: the full benefits of the Internet and VPN solutions are not always easily achieved by the enterprise alone. Therefore, enterprise VPN planners can benefit from foresight to the managed service options that are available to them.

The Managed Services Scenario

Many factors influence the enterprise to consider outsourcing their VPN needs. First is the growing distraction from core business that building and maintaining a network imposes on the enterprise. As a result, many enterprises choose not to invest in the global infrastructure that true eBusiness applications will ultimately entail. It is simply too costly for them to build, own and operate these global networks on a 24x7 basis. In addition, managing many site-to-site and remote access security policies can be administratively complex, requiring a new level of expertise that may not be easily added to the staff. Further, deploying and managing VPN client software for hundreds or thousands of remote users is another administrative challenge.

In fact, the staffing challenge alone will motivate many small to mid-sized companies to leverage a service provider's VPN outsourcing option. Even large organizations will be challenged to scale their operations to compete in this global eBusiness economy.

The key benefits of a managed services solution include:

- Rapid, global deployment – Adding new sites or new users to the VPN managed service can be a simple matter of the provider installing an access link with the CPE equipment or secure client software. The provider takes responsibility for any site and backbone level provisioning required.
- Scale - The Internet offers unmatched geographic coverage, providing the infrastructure and operational capacity necessary to operate on a global, 24x7 basis. Customers gain an immediate ability to scale beyond internally constrained resources by leveraging service provider backbone and network management resources.
- The strategic advantage - Given the virtual enterprise imperative, use of a managed service may determine whether or not an enterprise can compete as a global eBusiness player.
- Reduced costs - The cost of ownership advantage is compelling, and comes not only from leveraging a public rather than private network for wide area communications, but also from the reduced staffing. The Telechoice survey found that the leverage gained through outsourcing yields roughly 15 times greater staff power - the ratio of support staff to users in self-managed VPNs is 1:150 but in outsourced VPNs will reach 1:2,300.
- High availability - Managed, end-to-end VPN services with full QoS and SLA performance guarantees can support the most demanding business applications.

The Hybrid Approach

A combination of self-managed and outsourced VPN services may give the enterprise the best of both worlds. For rapid deployment and global scalability, the enterprise can leverage the service provider infrastructure while still maintaining control over VPN access and security administration.

©2000 Lucent Technologies, Inc.

All of the key benefits of the DIY and the managed services scenarios can be incorporated in a hybrid VPN model. Service provider SLAs can be crafted to meet the requirements of multiple VPN applications under the umbrella of a hybrid approach. It is also possible for multiple partners to cooperate with each other in providing a complete solution, each bringing unique expertise, regional scope or eBusiness capabilities to the overall solution.

Interoperability and flexibility is derived from IP standards that allow the different players to operate jointly across a unified VPN architecture. For most organizations, VPN planning over the mid to long-term will be a matter of factoring the different elements of a hybrid VPN solution.

II. What To Look For In VPN Solutions

It's important to note that a managed service can be implemented either as a premises-based or as a network-based VPN service. A premises-based solution includes customer premises equipment (CPE) that allows end-to-end security and Service Level Agreements (SLAs) that include the local loop as a key differentiator.

A network-based VPN, on the other hand, is provisioned mainly by equipment at the service provider's PoP, and does not provide equivalent guarantees over the last mile. Secure VPNs that deliver robust, end-to-end SLAs will demand a premises-based solution built on an integrated family of secure VPN platforms.

A complete, fully integrated product line

Given the need to communicate securely with corporate users, partners and customers via site-to-site or remote access links with varying degrees of infrastructure already in place, it is important that the VPN product line include a fully integrated and managed complement of technologies and products.

A VPN can be constructed using purpose-built VPN routers or by attaching VPN gateways as an adjunct to existing routers. Next generation VPN routers are purpose-built to deliver tightly integrated IP routing, security, firewall, and bandwidth management features at leadership performance and scale. A VPN gateway is typically a low-cost appliance that provides functionality such as tunneling, encryption and firewall services as an overlay to a previously installed, currently stable IP network.

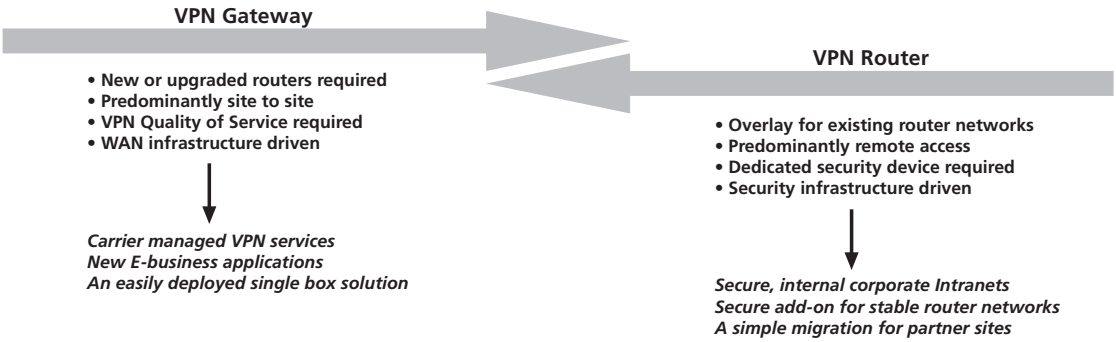


*Figure 3—**VPN router and gateway solutions.** Greatest breadth of application coverage.*

©2000 Lucent Technologies, Inc.

While the VPN router is an easily managed single box solution that is ideal for deploying new VPN applications and sites, the VPN Gateway provides a simple migration path to secure VPN services for an existing network. As a dedicated security device, the VPN Gateway can also be installed to provide a separately managed high security perimeter for the enterprise.

In both cases the product line must be broad enough to address the distinct price and performance needs of very large headquarter sites, regional offices and also small office/remote office locations.

An IPSec client that is fully interoperable with the entire product line and centrally managed for ease of deployment and scale must also be included with the VPN product portfolio.

Centralized, Policy-enabled Management

Centralized policy management is the key to building robust, large-scale VPN solutions. By allowing VPN configuration and security policies to be distributed holistically but controlled centrally, policy management greatly simplifies VPN provisioning and administration. Services are no longer provisioned box-by-box, but instead can be delivered and easily adapted to support a range of applications over a policy-managed VPN infrastructure.

Deployment is simplified and network access is under the control of enterprise administrators - they can define policies and apply them to support many different levels of access enforcement across the network. For example, sites can be configured to communicate with encryption for certain Intranet applications, more openly for normal Internet use, and with user authentication for remote access.

VPN security policies are based on the Internet Engineering Task Force's (IETF) IP Security (IPSec) standard. IPSec comprises multiple Internet RFCs that address the confidentiality, integrity, authentication and access control of IP packets. No longer a pending draft, IPSec is fully approved, tested and being used today to support large-scale eBusiness solutions.

Leadership Security and Performance

Because a VPN product separates sensitive data and networking resources from hostile networks (such as the Internet), a VPN product must be every bit as strong as a firewall. Strong authentication, cryptography, X.509v3 digital certificates, and ICSA-certified firewall functions ensure that VPNs protect data privacy.

VPN security policies are based on standards that are robust, stable and being used today to support large-scale eBusiness solutions. IP Security (IPSec) is the Internet Engineering Task Force's (IETF) Internet protocol security standard. It is the standard for IP security.

Service level agreements are another key feature of end-to-end VPN solutions, equal to network security in importance. SLAs provide concrete performance metrics to ensure that VPNs support reliable business services. Performance monitoring also generates valuable data for network planning and applications support. SLAs should cover not just individual links, but overall performance between all of a customer's sites.

Quality of service (QoS) capabilities are also important criteria. VPN products with robust QoS features can support mission-critical business applications. Service quality is crucial to enterprise requirements for prioritized traffic and managed access to the VPN.

©2000 Lucent Technologies, Inc.

Platform Features

Key attributes to look for in a premises-based platform architecture include:

Standards Compliance: The standard for secure VPNs is IPSec, an IETF standard. Managed VPN service with 128-bit IPSec encryption is not deployed by all providers. Don't be sidetracked with proprietary security technologies or transitioning promise.

Firewall Security: The VPN solution is as critical as a firewall, so the service platform should be manageable in tight synchronization with other enterprise firewall and intrusion detection systems. The platform should include a tightly integrated, ICSA-certified firewall, not "firewall filters" or "access control lists" that were shoehorned into 3rd-party firewalls.

Authentication: For strong user authentication, the platform should support SecurID tokens or X.509 digital certificates. Avoid using general purpose operating systems as a foundation for VPN devices; they can be full of security holes.

Multiple Certificate Authority (CA) Support: Don't be tied to a proprietary Certificate Authority (CA) or certificate enrollment protocol. Support for multiple CAs (such as Entrust and VeriSign) allows net managers to select the best of breed in Public Key Infrastructure (PKI) technology.

Hardware-Accelerated Encryption: The processing required to perform encryption and decryption is intensive, particularly when performing automated key exchange. For high-speed applications (e.g., T-3), the service platform should feature hardware-accelerated encryption. For lower-speed applications, software-based encryption may be suitable.

Scalability: Most enterprises face growing or changing networking needs, including faster connections and increasing locations. The ability to grow a VPN solution without wholesale hardware/software replacement is important. The architecture should be able to support at least dozens, if not hundreds, of VPN gateways and thousands of VPN clients.

III. The Lucent Secure VPN Portfolio

Lucent's Secure VPN portfolio of products and management systems is the industry's most comprehensive framework for building premises-based VPN services. The portfolio includes IPSec client software, VPN routers, VPN gateways and firewalls, all with centralized policy management for easy provisioning and extensible customer control of robust service features.

A single customer may require products spanning the full range of the Secure VPN portfolio to meet various needs. The portfolio breadth and depth allows optimal configurations with a choice of service platforms, security options, performance levels, management capabilities, and business models - whether DIY, outsourced, or a combination of both.

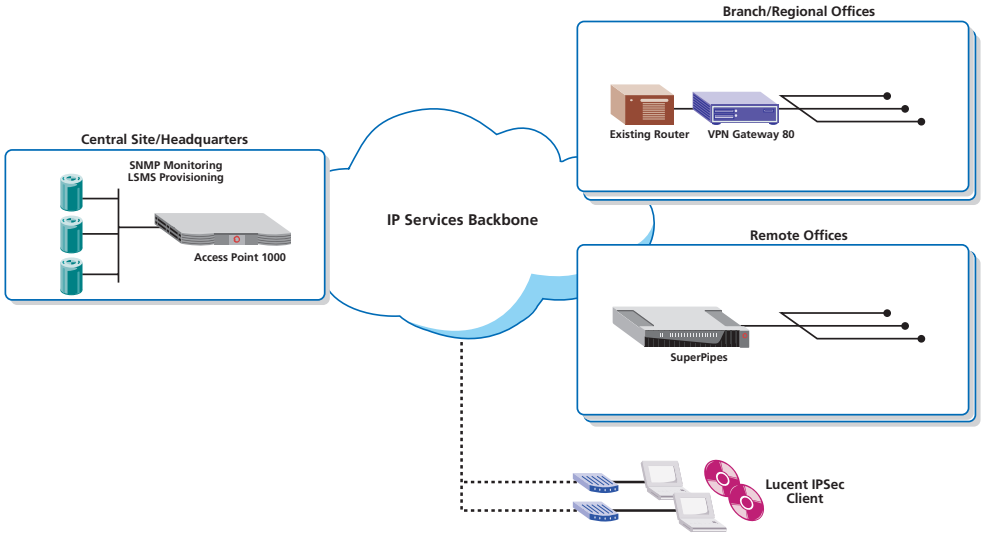
Lucent VPN Gateway and Client

Priced starting at $2,000, Lucent VPN gateway products provide IP networks with a cost-effective VPN overlay that includes robust firewall and hardware encryption services. Gateway management is centralized and scalable to support thousands of IPSec software clients on mobile and remote user PCs.

VPN Gateway

Strong firewall integration is a key feature in this class of product. A highly secure ICSA- and NSA-certified firewall is included in Lucent's VPN gateway, along with strong authentication and access control using best-of-breed standards-based solutions.

©2000 Lucent Technologies, Inc.



Applications:

- Site-to-Site Intranet: connecting various enterprise locations, such as branch offices and headquarters, using low cost IP networks instead of dedicated circuits or frame relay services.
- Secure Remote Access: more than just analog or ISDN access to your enterprise network...can also take advantage of high speed cable modem, satellite, and DSL access.
- Partner Extranet: quick setup and teardown of secure connections to extranet business partners, suppliers, customers and government agencies.

Products:

- Access Point, SuperPipe and Pipeline Routers: Integrated VPN routers
- Lucent VPN Gateway: Secure VPN gateways
- Lucent IPSec Client: Integrated VPN Client software
- Lucent Security Management Server (LSMS) and QVPN Builder: Centralized policy-based management

Security Standards

- IPSec: with 3DES, DES and RC4 encryption
- Authentication: SHA-1 and MD5
- Key Management: Automated key management using Internet Key Exchange (IKE) and Public Key Infrastructure (PKI)
- Digital Certificates: X.509v3 digital certificates and Secure Socket Layer (SSL) encryption for secure Web administration
- Firewall: ICSA-certified firewall integration

*Figure 4—**Secure VPN applications, products and standards.***

The VPN gateway 201 is a purpose-built platform using hardware encryption to sustain 75 Mbps 3DES throughput with up to 2,000 simultaneous tunnels. Non-encrypted throughput is 125 Mbps with over 100,000 simultaneous tunnels. Lucent VPN gateways use a proprietary operating system that eliminates standard OS security holes. Active defenses can be heightened with Lucent's integrated intrusion detection and security auditing systems.

IPSec Client

For mobile workers, telecommuters, and single computer locations, Lucent's software-based IPSec Client provides a powerful, affordable VPN solution. The IPSec Client includes encryption (DES/3DES) and authentication (MD5/SHA1), and supports RADIUS or SecurID one-time token-based authentication systems. When an IPSec Client connects to any gateway in the Secure VPN portfolio, it automatically and transparently authenticates the user and executes security policies. For example, policies may dictate which connections are permitted, which should be encrypted and sent via secure tunnel, and which may be passed in the clear. Configurations can be centrally managed to ensure strict enforcement of access privileges via the Lucent Security Management Server (LSMS)

©2000 Lucent Technologies, Inc.

Access Point and Pipeline/SuperPipe VPN Routers

The Access Point and Pipeline/SuperPipe routers combine routing, bandwidth management, VPN and firewall functions in an integrated service platform that has been purpose-built for industry leading performance, price/performance, scalability and ease of management.

Pipeline and SuperPipe

Ideal for branch offices, telecommuters and client or partner sites, the Pipeline family of VPN routers offer superb price/performance, low cost of ownership, and scalability to match deployments ranging from single-user home offices to multi-user branch offices of virtually any size.

Pipeline and SuperPipe combine integral WAN access, routing, IPSec tunneling and encryption, robust authentication services and an integrated firewall. With centralized, automated VPN policy management through the Lucent Security Management Server (LSMS), including both IPSec and Firewall policy management, Lucent VPN routers reduce the complexity and cost of ownership for large-scale service deployment.

Access Point

For larger sites that require the performance and scalability to support heavy traffic or thousands of VPN tunnels, Access Point VPN routers are an ideal platform. Access Point routers can be used with any WAN technology - IP, Frame Relay, or ATM - and support both site-to-site and remote access VPN applications. An integrated hardware encryption accelerator achieves traffic forwarding rates of up to 90 Mbps using DES or 3DES encryption.

Lucent also delivers IP quality of service (QoS) leadership with Access Point's class-based queuing (CBQ) technology. CBQ divides traffic into a hierarchy of classes and then assign each class a set of bandwidth attributes that define access privileges at the boundary between enterprise and VPN networks. Service levels can be created, enforced, and tariffed to improve IP network usage. Access Point is fully DiffServ-compliant, achieving QoS signaling through the current IETF-defined industry standard.

Policy Management

At the core of Lucent Secure VPN portfolio is an integrated, centralized VPN policy management platform, the Lucent Security Management Server (LSMS). The LSMS interfaces with RADIUS and SecurID user-authentication servers. It also handles public key infrastructure and Certificate Authority (CA) management of X.509 digital certificates. LSMS provides extensive auditing, logging and alarm capabilities, and is integrated with Lucent's RealSecure™ intrusion detection system for enhanced security.

LSMS and QVPN Builder

LSMS has proven itself as a centralized provisioning tool for enterprises building large-scale remote access VPNs. A single LSMS can manage hundreds of VPN Gateways, Pipeline and SuperPipe VPN routers, and thousands of IPSec Clients - up to 24,000 VPN tunnels can be managed at once.

Access Point QVPN Builder is a policy management application running under the LSMS system that has been specifically optimized for site-to-site provisioning of enterprise VPNs. With centrally managed VPN profiles, firewall rules, and QoS policy definition, QVPN Builder enables large-scale VPNs to be deployed quickly and at low cost. Lucent's VPN configuration and policy-based management capabilities lead the industry and draw their strength through the integration of LSMS and QVPN Builder.

©2000 Lucent Technologies, Inc.

IV. Conclusion

VPNs are a fundamental solution for achieving the global connectivity that companies require in order to leverage their reach as virtual enterprises with an extended community of partners, customers and employees.

Internal business drivers compel some organizations to build their own VPNs while others outsource their solutions either whole or in part, but, either way, enterprise VPN planners will benefit from understanding the managed service options that are available. A combination of self-managed and outsourced VPN services may in fact give the enterprise the best of both worlds. For rapid deployment and global scalability, the enterprise can leverage service provider infrastructure while still maintaining control over VPN access and security administration.

In choosing a VPN solution it's important to consider a complete product line that includes not only core platforms but also integrated client support and centralized policy management for unified, easily provisioned services. The ability to extend granular administrative privileges and to carve an IP network into unique customer-managed zones is a key enabler of VPN solutions, but it is not common to all service platforms. Lucent's industry-leading SecureVPN portfolio demonstrates the end-to-end VPN dexterity and robustness that allows enterprise customers and their service providers to build secure solutions for any business need.

Entire contents copyrighted by Lucent Technologies, Inc. Unauthorized redistribution, electronic or otherwise, without prior written approval of Lucent Technologies, Inc., is prohibited by law. Requests for permission to copy or distribute Lucent Technologies, Inc., 50 Nagog Park, Acton, MA 01720 USA

Lucent Technologies, Inc.
50 Nagog Park
Acton, MA 01720 USA
Tel: 978-263-0600
Fax: 978-263-6980
www.lucent.com

©2000 Lucent Technologies, Inc.