Lucent Technologies
Bell Labs Innovations



WHITE PAPER

Secure VPN Strategies for the Enterprise and Service Provider

Leveraging the MultiService Alliance VPN Segment (MAP-VPN)

Ron Silver
Product Marketing Manager

05-99
08/00

Table of Contents

1. About the MAP-VPN Alliance 1

How Partners and Customers Benefit 1

2. Today's VPNs for the Enterprise 2

VPN Services 2

Self-Managed, Outsourced, or Both? 3

What Enterprises Should Look For in a VPN Solution 5

3. Today's VPNs for the Service Provider 8

A Win-Win Scenario for Providers and Enterprise Customers 9

What Does "Managed" Mean? 10

Managed Service Opportunities and Challenges 10

Enabling Customer Control Through Policy Management 12

What To Look For in a VPN Solution 12

4. Lucent VPNWorX™ and Secure VPN Portfolio 15

The Lucent VPNWorX Portfolio 15

The Lucent Secure VPN Portfolio 15

Lucent VPN Firewall Brick and IPSec Client 16

Policy Management 17

5. MAP-VPN Partner Solutions 19

Four Major Technology Categories 19

Unique Internet Service Provider VPN Access Solutions 19

MAP-VPN Partner Fit 21

MAP-VPN Technology Partner Integration 21

Infrastructure 28

5. Conclusion 31

©2000 Lucent Technologies, Inc.

1. About the MAP-VPN Alliance

The Lucent MultiService Alliance, VPN Segment (MAP-VPN) offers a multifaceted approach to developing VPN solutions, in a cooperative win-win environment that benefits all participating partners, resellers, and ultimately, the enterprise.

The MAP-VPN provides customers with a combination of best-in-class products for virtual private network (VPN)/security applications. These products, developed by Lucent technology partners (TPs), have been integrated* into Lucent's Secure VPN product portfolio, along with a continuum of operational models supported directly by Lucent, Lucent's value-added resellers (VARs), selected professional service providers (PSPs), and selected national and international Internet service providers (ISPs).

As shown in Table 1, cross-dependencies exist among MAP-VPN partners and customers. For example, TP partners and PSP partners are in a position to support resellers by enabling resellers to bundle more products and services into their VPN-related solutions. These added capabilities strengthen resellers' positions as "one-stop shops," while simplifying choices for their enterprise or ISP customers. Resellers can also co-market with a MAP-VPN ISP to further simplify a customer's choices. Also, PSPs are in a position to support direct-to-enterprise sales, reseller-to-enterprise sales, and ISP-to-enterprise sales.

MAP-VPN Partners and Customers

Lucent Partners			Lucent Customers	
TP	PSP	ISP	Reseller	Enterprise

Table 1

How Partners and Customers Benefit

Technology Partners (TP): Expand the opportunity to sell application products through the MAP-VPN cooperative marketing programs and reseller incentives. In turn, technology partners provide backup support to PSPs to help assure a successful installation.

Professional Service Providers (PSP): Expand the opportunity to sell professional services through MAP-VPN cooperative marketing programs. With this increased exposure to Lucent's sales channels, PSPs have greater opportunity to increase revenues.

Internet Service Providers (ISP): Expand the opportunity to sell network access and VPN managed services by leveraging Lucent's sales channels and Lucent's expanding suite of VPN solutions.

Value-Added Resellers (VARs): Increase sales of VPN-related products and services by enhancing VPN offerings with bundled application products and professional services. In this way, resellers become one-stop-shops, which can increase revenues and profits.

Enterprises: Become the ultimate beneficiary, because they can take advantage of simplified sourcing and business models to achieve the most cost-effective and optimal VPN solution.

**To ensure interoperability and reliability, Lucent's Reflective Protocol Tool Kit, an applications programming interface (API), has been used to integrate many of these applications, followed by thorough testing.*

©2000 Lucent Technologies, Inc.

2. Today's VPNs for the Enterprise

VPN Services

eBusiness opportunities are driving enterprise demand for flexible and secure wide-area communications. In addition, Internet connectivity and IP networking advances are intensifying companies' needs to exchange information with customers, suppliers, and business partners anywhere in the world. These demands are rapidly growing beyond the scope of traditional network solutions. As businesses leverage their reach in what is now commonly referred to as the "virtual enterprise," IP-based VPN solutions are proving to be one of the most highly effective solutions for achieving global connectivity.

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

Global VPN and Managed Services Growth

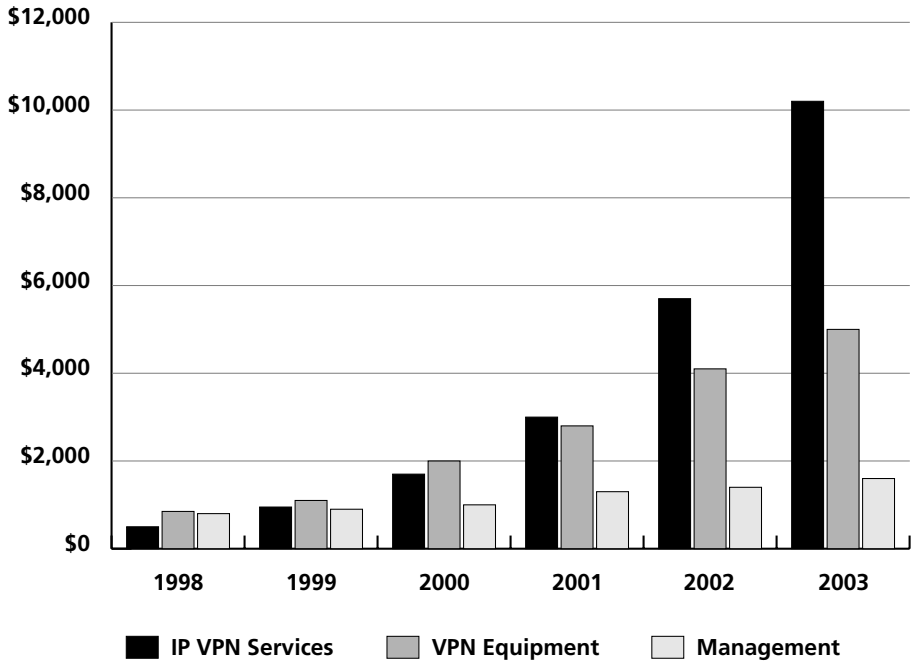


Figure 1

While enterprises acknowledge the critical role the Internet and IP VPNs will play in their strategic eBusiness initiatives, they face a range of choices for implementing their VPNs. The options range from "do-it-yourself" (DIY) VPNs that are fully built, owned, and operated by the enterprise, to VPNs that are fully outsourced to a partner. In the near term, it is generally believed that enterprise-operated and managed VPN services will hover around a 50/50 split, including hybrid approaches.

©2000 Lucent Technologies, Inc.

Types of VPNs Being Implemented in 1999/2000

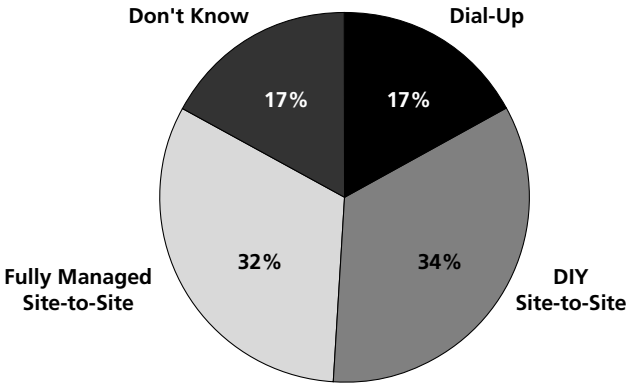


Figure 2

Self-Managed, Outsourced, or Both?

Increasingly, enterprises are assessing their VPN implementation options across a spectrum of DIY, fully outsourced, or hybrid models. Each approach offers a unique business advantage.

- **Do-It-Yourself:** This option operates over a public network facility (most commonly the Internet) using equipment owned and operated by the enterprise. Its greatest benefit to the enterprise is the degree of flexibility and control it offers—over VPN deployment, administration, and adaptability or change.
- **Fully Outsourced:** This managed service could be implemented by a collection of partners, including an ISP and a security integration partner. Its advantages include quick deployment, easy global scalability, and freedom from overhead network management.
- **Shared Management:** With this hybrid approach, a partner may take responsibility for major elements of infrastructure deployment and management, but the enterprise 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 corporations reserve the option to outsource part or all of their VPNs at some point along the way, they are investing in the resources necessary for the initial trial, then scaling to a broader set of applications on their own.

Most enterprises retain VPN ownership due to a business-centered need to maintain control of key policies or administrative tasks. For example:

- For some enterprises, the corporate charter requires the organization to retain sole control over all elements of network security.
- Other enterprises rely on their networks as strategic elements of their businesses. In today's competitive environment, they want to maintain a level of control that will enable immediate response times and rapid adaptation to changing customer demands and business requirements.

©2000 Lucent Technologies, Inc.

In some cases, enterprise customers may start with a DIY strategy, then migrate to a managed service. As part of this process, many corporations are asking their equipment vendors to include an ISP and a security expert in planning discussions—to help assess how their VPN solution might migrate over time. Once the core VPN is in place, with the appropriate definition and policies, then the best way to extend the VPN may be with a global managed service partner.

In fact, recent Telechoice research found that outsourcing is the number-one change today's enterprise VPN managers have planned for their DIY networks. The reason is straightforward: 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 considering all the managed service options available to them.

The Managed Services Scenario

Many factors influence enterprises to consider outsourcing their VPN needs. Building and maintaining a network takes time, money, and effort away from their core businesses. As a result, many enterprises are not investing in the global infrastructure that true eBusiness applications will ultimately demand, because 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 is unfamiliar to the current staff. Deploying and managing VPN client software for hundreds or thousands of remote users is another administrative challenge.

In fact, staffing demands alone may motivate many small- to mid-sized companies to leverage a service provider's VPN outsourcing option. Even for large organizations, the operational expansion needed to compete in this global eBusiness economy presents a formidable challenge.

The key benefits of a managed service solution include:

- **Rapid, global deployment:** Adding new sites or new users to VPN managed services can be a simple matter of the provider installing an access link with customer premises equipment (CPE) 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 capacity necessary to operate on a global, 24x7 basis. By leveraging a service provider backbone and network management resources, an enterprise can immediately expand beyond its own limited resources.
- **The strategic advantage:** Given the virtual enterprise imperative, use of a managed service may be the only way an enterprise can compete as a global eBusiness player.
- **Reduced costs:** The cost of ownership advantage is compelling, and comes by leveraging a public, rather than private, network for wide-area communications and by reduced staffing requirements. A 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, it can reach 1:200–300.
- **High availability:** Managed, end-to-end VPN services with full Quality of Service (QoS) and Service Level Agreement (SLA) performance guarantees can deliver reliable support for 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. The enterprise can leverage the service provider infrastructure for rapid deployment and global scalability, while maintaining control over VPN access and security administration.

©2000 Lucent Technologies, Inc.

All the key benefits of the DIY and managed service scenarios can be incorporated in a hybrid VPN model. Service provider SLAs can be crafted to meet the requirements of multiple VPN applications, and multiple partners can cooperate in providing a complete solution, each bringing unique expertise, regional scope, or eBusiness capabilities to the overall solution.

Interoperability and flexibility are 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 coordinating the various elements of a hybrid VPN solution.

What Enterprises Should Look for in a VPN Solution

It's important to note that a managed service can be implemented either as a premises-based solution or a network-based VPN service. A premises-based solution includes CPE that allows end-to-end security and SLAs that include the local loop. These end-to-end guarantees of quality are key differentiators.

A network-based VPN, on the other hand, is provisioned mainly by equipment at the service provider's point-of-presence (PoP), so it does not provide equivalent guarantees over the last mile. For a secure VPN that delivers robust, end-to-end SLAs, an enterprise must demand a premises-based solution built on an integrated family of secure VPN platforms.

A Complete, Fully Integrated Product Line

Today's enterprises need to communicate securely with corporate users, partners, and customers, via site-to-site or remote access links, while leveraging their existing infrastructure. As a result, it is important for a VPN product line to include a fully integrated and managed complement of technologies and products to meet these highly specific and complex requirements.

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, tunneling, encryption, security, firewall, and bandwidth management features with leading 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.

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 selection of products must be broad enough to address the distinct price and performance needs of very different locations—including large headquarters sites, regional offices, and small remote office locations.

An IP Security (IPSec) client, fully interoperable with the entire product line and centrally managed for ease of deployment and expansion, should 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. It provides a powerful combination of centralized control, along with broad-based distribution of VPN configuration and security policies. This approach greatly simplifies VPN provisioning and administration, because services are no longer provisioned box-by-box. Instead, they can be delivered and easily adapted to support a range of applications over a policy-managed VPN infrastructure.

As a result, deployment is simplified, and network access is under the control of enterprise administrators. They can define policies and quickly apply them to support many different levels of access enforcement across the network. For example, sites can be configured to

©2000 Lucent Technologies, Inc.

communicate with different levels of security, depending on the application—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 (IETF) IPSec standard. IPSec comprises multiple Internet Requests for Comment (RFCs) that address the confidentiality, integrity, authentication, and access control of IP packets. No longer a pending draft, IPSec is fully approved, tested, and currently used to support large-scale eBusiness solutions.

Leading Security and Performance

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

VPN security policies are based on robust, stable, industry-recognized standards that are used today to support large-scale eBusiness solutions. IPSec is the IETF's Internet protocol security standard. It is the standard for IP security.

Service Level Agreements (SLAs) are another key feature of end-to-end VPN solutions, equal in importance to network security. 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. For both these purposes, SLAs should cover overall performance among all enterprise sites, not just individual links.

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

Platform Features

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

Standards Compliance: While IPSec, an IETF standard, is the industry-recognized protocol for secure VPNs, not all providers deploy a managed VPN service with 128-bit IPSec encryption. Enterprises should avoid proprietary security technologies or transitioning promises that don't offer the same capabilities as the IPSec standard.

Firewall Security: A VPN solution is as critical as a firewall, so the VPN 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 have been shoehorned into third-party firewalls.

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

Multiple Certificate Authority (CA) Support: Enterprises should also avoid being tied to a proprietary certificate authority (CA) or certificate enrollment protocol. Support for multiple CAs, such as Entrust, RSA, and VeriSign, allows network managers to select the best-of-breed in public key infrastructure (PKI) technology.

©2000 Lucent Technologies, Inc.

Hardware-Accelerated Encryption: The processing required to perform encryption and decryption is intensive, particularly when performing automated key exchange. For high-speed applications, such as T-3, the VPN 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 numbers of locations. A VPN solution must be able to handle these changes without wholesale hardware or software replacement. The architecture should be able to support at least dozens, if not hundreds, of VPN gateways and thousands of VPN clients.

Flexibility: A VPN solution should include products that can be migrated from a DIY to a managed service scenario. The enterprise or the service provider should not have to replace or modify the installed products just because, for example, the management of the devices moves from enterprise control to service provider control.

©2000 Lucent Technologies, Inc.

3. Today's VPNs for the Service Provider

With eBusiness opportunities driving demand for more flexible and secure wide-area communications, enterprise customers are forecast to spend more than $14 billion annually on IP-based VPN equipment and services by 2003. As the growing need for connectivity and IP networking advances push traditional network solutions to their limits, IP-based VPN services with guaranteed QoS and SLAs are proving to be among the most highly effective solutions for enterprise connectivity.

One-third of companies that rely on wide-area communications are already using IP-based VPN services, either in production or in trials, according to market research completed by Telechoice, Inc. in late 1999. The VPN market is accelerating and one of its most striking trends is the shift to outsourced VPN solutions. Telechoice found that outsourcing is the number-one change that today's enterprise VPN managers have planned for their DIY networks.

Early VPN adopters and most enterprise pilot projects started with DIY solutions. Now, many have decided they would rather use managed VPN services, instead of handling their VPNs in-house. The split between home-grown VPNs and outsourced services was roughly 3:1 in 1999. But with increasing demand, the level of outsourcing is likely to double within 18–24 months.

VPNs Growing Fast, Worldwide

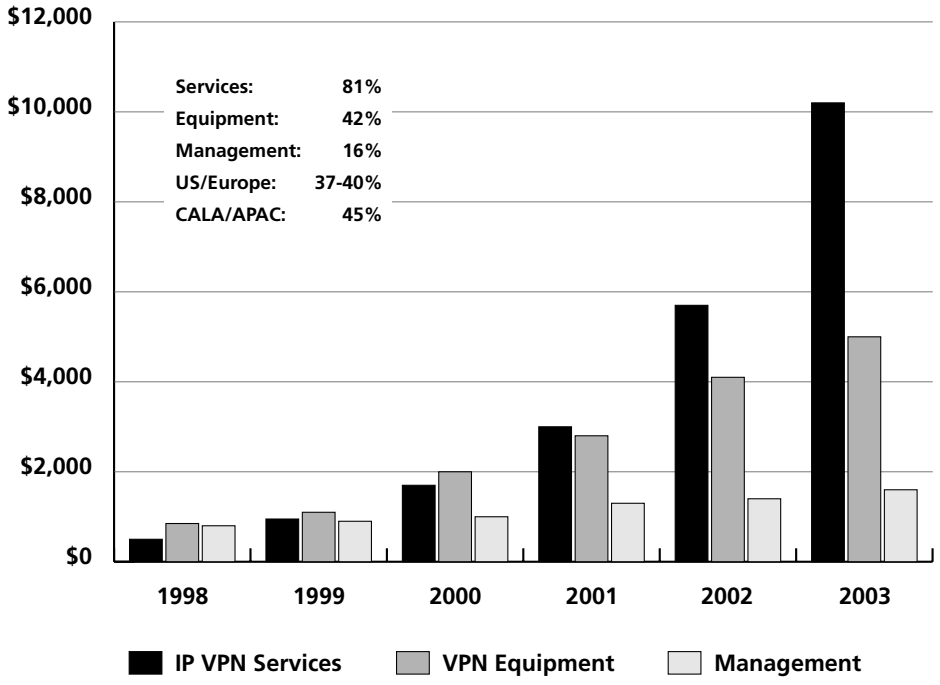


Figure 3

As the leading manufacturer of VPN infrastructure solutions for both service providers and enterprises, Lucent Technologies engages in VPN planning with many potential users. Increasingly, customers want these discussions to include ISPs and backbone carriers, as well as experts on Internet security or VPN integration, all joined by the technology vendor.

Their purpose from the start is to explore and understand the trade-offs between DIY VPNs and the various flavors of outsourced VPN managed services. The reason for this growing interest in

©2000 Lucent Technologies, Inc.

outsourcing is straightforward: the full benefits of the Internet and VPN solutions are not always easily achieved by the enterprise alone. The networking scope, scalability, and infrastructure needed to support global eBusiness and to administer service 24x7 is often more than an enterprise is willing to invest in or manage. As a result, today's enterprise VPN planners are choosing to explore the managed services that are available and the benefits they can provide at the beginning of the planning process.

A Win-Win Scenario for Providers and Enterprise Customers

Enterprise customers have several motivations for outsourcing all or part of their VPN solutions to service providers, including an overall desire to focus on core business competencies and improve network performance.

Enterprise Customer Benefits

- **Flexibility and scalability:** Adding new sites or new users to VPN managed services can be a simple matter of the provider installing an access link with the CPE or secure client software. The provider takes responsibility for any site and backbone-level provisioning required. An optimal VPN design uses a single connection for private intranet, semi-private extranet, and public Internet access. This integration saves money for enterprises, but is equally advantageous for service providers, allowing them to cost-effectively expand their services across today's private/public network boundaries.
- **Rapid deployment and global reach:** VPN outsourcing gives enterprise customers a fast, easy way to expand communications beyond the limits of their existing networks. It quickly connects individual users and multiuser offices worldwide, and provides support for popular applications and protocols. Enterprises gain immediate scalability by leveraging the service provider's backbone, instead of building their own. The Internet offers unmatched geographic coverage, providing the infrastructure and capacity necessary to operate on a global, 24x7 basis.
- **High performance:** Managed, end-to-end VPN services with full QoS and SLA performance guarantees can maintain the highest levels of availability—and support the most demanding business applications.
- **Reduced operating cost:** Customers avoid the cost and complexity of hiring technical experts and maintaining increasingly complex technologies. Instead, they can leverage the outsourcing partner's expertise and dedicated resources.

Service Provider Benefits

Service providers offer VPN managed services for a variety of reasons. Primarily, they present an outstanding opportunity to expand a provider's range of service offerings and broaden relationships with existing customers.

- **New revenue generation:** VPN outsourcing can incorporate an array of value-added services, such as Web hosting, application hosting, and eCommerce support, which demand the industry's most capable and scalable multiservice VPN platforms.
- **Rapid deployment:** With no change in existing core networks, new CPE-based services can be deployed rapidly, speeding time-to-market and helping to capture market share.
- **Differentiated service offerings:** Next-generation capabilities, such as QoS and SLA-aware routing and switching, can give providers a competitive advantage.
- **Strategic relations:** Providing value-added service, not bandwidth, brings the provider into more long-term strategic relationships with customers. VPNs can be the entry point for other value-added services over time.

©2000 Lucent Technologies, Inc.

What Does “Managed” Mean?

Within their spectrum of "managed" services, providers can manage, monitor, and act to protect VPNs in a number of ways. They can monitor equipment and connection health, implement customer-requested changes, monitor security status, and initiate defensive measures against VPN attacks.

The following table describes some key service components that can be included in managed VPNs:

Components of a Managed Solution

Typically Included	Other Possible Components
■ Customized Solution Design	■ Help Desk/Remote User Support
■ Access and Connectivity	■ Security Policy Development
■ Equipment Lease or Sales	■ Extranet Setup
■ Equipment Configuration and Installation	■ Export Management Services
■ CPE Monitoring and Change Management	■ Managed Security/Authentication
■ Service Level Agreements	■ Secure Hosting and Applications
■ Client Software	

Table 2

Customized solution design includes all aspects of connectivity to enterprise sites, customers, suppliers, and remote users. Configuration and installation of equipment, including client software distribution, is a great benefit that eliminates the need for the enterprise to master new management platforms and configuration tools in order to deploy a network solution.

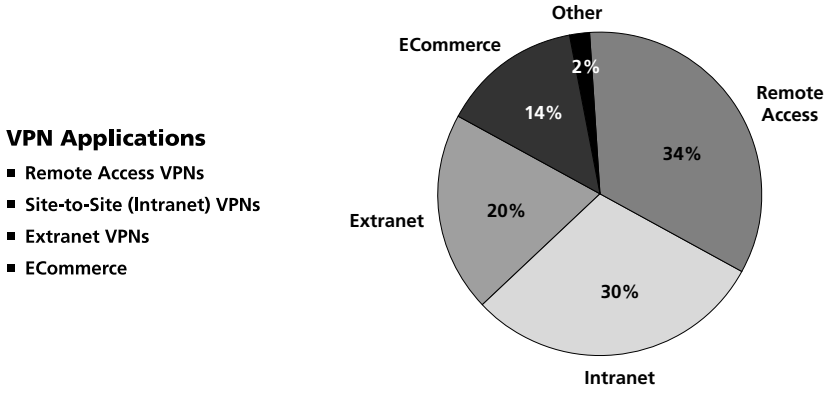
Most importantly, SLAs ensure that network application needs will be met. Not all VPN equipment and services provide equivalent SLA capabilities. For example, some SLAs do not include the local loop, so end-to-end SLAs are critical differentiators for VPN providers. SLAs built around availability and connection uptime are important considerations for enterprises that need maximum reliability.

Managed Service Opportunities and Challenges

Applications supported by VPNs fall into four main categories: enterprise site-to-site, enterprise remote access, business-to-business extranet, and consumer-oriented eCommerce.

©2000 Lucent Technologies, Inc.

VPN Applications



Source: TeleChoice, Inc.

Figure 4

Two primary factors influence enterprises to consider outsourcing their VPN needs. First, building and maintaining a network takes time and money away from their core businesses.

As a result, many enterprises are not investing in the global infrastructure that true eBusiness applications will ultimately demand. It is simply too costly for them to build, own, and operate these global networks on a 24x7 basis. For many enterprises, outsourcing provides a more secure, easily managed network solution than they could afford to build themselves. Second, outsourcing options have expanded greatly in the past year. Many providers now offer managed services that include guaranteed wide-area performance and, in some cases, end-to-end SLAs, so customers are finding a broader range of VPN services that will support their business requirements.

The global accessibility and flexibility of VPNs raise security issues that are beyond the scope of many enterprises. Managing user authentication and VPN access privileges can be difficult, given the number of users involved. Deploying and managing VPN client software for hundreds or thousands of remote users is another challenge.

Scalability is the key challenge of VPN security management. Deploying and managing a large number of security definitions across a variety of site-to-site and remote access configurations can be highly complex. As VPNs grow, PKI, Internet Key Exchange (IKE), and user authentication protocols, such as RADIUS, become difficult to manage. The required management skill can also be difficult to obtain. For small organizations, these issues are too costly and distract from core business; and for large organizations, the scale can be so large, both geographically and technically, that outsourcing is the best answer. When assessing whether to handle these challenges in-house or choose outsourcing, the key questions include:

- Can the organization secure (and retain) IPSec, IKE, and PKI expertise in-house?
- Does management have the required legal knowledge of export and encryption regulations?
- Can the organization provide 24x7 network deployment and support teams? Globally?
- Is there an expanding equipment and personnel budget?

IP security expertise is expensive. For that reason alone, many small- to mid-sized companies would leverage a service provider's VPN outsourcing option. Telechoice found that the leverage gained through outsourcing yields roughly 15 times greater staff power. The ratio of support staff to users in DIY VPNs is 1:150, but in outsourced VPNs, it can reach 1:200–300.

©2000 Lucent Technologies, Inc.

Enabling Customer Control Through Policy Management

As enterprise customers turn to VPN outsourcing, many still want to define and maintain control over their network security policies. So, typically, they ask the service provider to assume network infrastructure and device management responsibility, while the enterprise administers its own VPN and firewall security. User authentication offers a good example of how this shared management environment works. In this case, the enterprise can define any range of security relationships among its users, while the service provider maintains service infrastructure to track and enforce those security relationships. Since one of the strong VPN selling points is easy accommodation of new users and business connections, enterprises expect to be able to configure access privileges themselves and to manage the bandwidth their users consume.

This ability to deliver VPN managed services that allow flexible levels of enterprise control is crucial to service providers. Just a few years ago all VPN services, including frame relay, were either DIY or difficult and time-consuming to configure when enterprise requirements changed. But today's IP-based VPN services live up to their full potential for responsiveness by delivering easy extension of enterprise control.

Two technologies are key enablers of shared VPN control. The first is centralized policy management, which allows VPN configuration and security policies to be distributed network-wide, but controlled centrally. This approach greatly simplifies VPN provisioning and administration, because services are no longer provisioned box-by-box. Instead, providers have a faster, streamlined method for delivering and adapting a broad mix of managed services over a policy-managed VPN infrastructure.

The second key support for shared VPN control is an architecture that enables providers to partition a network among different users, allowing various levels of administrative privileges. Today's VPN equipment allows IP networks to be carved into distinct customer security zones that permit flexible administrative and access configurations, without affecting other customers on the service provider's network. As a result, enterprises have greater control within their own VPNs.

These two enabling features provide a foundation for the most important advantages of VPNs. They allow enterprise customers to administer their networks directly, so they can accommodate daily changes without depending on the service provider's help desk for reconfiguration. Bandwidth can be monitored and managed according to SLAs; yet the burdens of deployment, network routing, and security management are removed. The bottom line for enterprise customers is faster deployment, more flexibility in change control, and an easily scalable network solution.

What to Look for in a VPN Solution

Security and Performance

Because VPN products separate sensitive data and networking resources from basically unsecure networks, such as the Internet, they must be every bit as strong as a firewall. Strong authentication, cryptography, X.509v3 digital certificates, NSA and ICSA-certified firewall functions ensure that VPNs protect data privacy.

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

SLAs are another key feature of end-to-end VPN solutions, equal in importance to network security. SLAs provide concrete performance metrics to ensure that VPNs support reliable business services, and their performance monitoring generates valuable data for network planning and applications support. For both these purposes, SLAs should address the overall performance among all enterprise sites, not just individual links.

©2000 Lucent Technologies, Inc.

QoS capabilities are also important criteria when choosing an appropriate VPN solution. VPN products that offer robust QoS features can support mission-critical business applications. These features can also meet enterprise requirements for prioritized traffic and managed access to the VPN. Finally, the VPN product set must seamlessly migrate from a DIY to a managed service scenario.

Premises-Based vs. Network-Based VPN

It's important to note the difference between premises-based VPN solutions and network-based VPN services. A premises-based solution includes CPE that allows true end-to-end security and performance management. 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.

Organizations that require secure VPNs, with robust SLAs and the ability to support various QoS requirements, will demand a premises-based solution. The key attributes to look for in premises-based platform architecture include:

- **Centralized Policy Management:** By controlling network security and QoS policies centrally, and distributing them to all VPN routers, appliances, and IPSec clients, a policy-managed service is easier to provision and use. The provider network becomes a unified system, not a collection of boxes and can support any set of flexible services anywhere on the network.
- **Strong 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, NSA and ICSA-certified firewall, not "firewall filters" or "access control lists" that were shoehorned into third-party firewalls. For strong user authentication, the platform should support SecurID tokens or X.509 digital certificates. General-purpose operating systems should be avoided as a foundation for VPN devices, because they can be full of security holes.
- **Standards Compliance:** IPSec is the industry-recognized IETF standard for creating secure VPNs. However, not all providers deploy managed VPN service with 128-bit IPSec encryption. Proprietary security technologies and transitioning promises simply don't meet the same standards.
- **Multiple Certificate Authority (CA) Support:** Proprietary Certificate Authority (CA) or certificate enrollment protocols limit a network manager's ability to choose leading VPN products across the network. With support for multiple CAs, such as Entrust and VeriSign, managers can make sure they select the best-of-breed in 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, such as T-3, the VPN 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 numbers of locations. The ability to grow a VPN solution without wholesale hardware and 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.
- **Flexibility:** A VPN solution should include products that can be migrated from a DIY to a managed service scenario. The enterprise or the service provider should not have to replace or modify the installed products just because, for example, the management of the devices moves from enterprise control to service provider control.

©2000 Lucent Technologies, Inc.

VPN Routers and Gateways

VPN functionality can be added to existing infrastructure either by deploying purpose-built VPN routers or by attaching VPN gateways to existing routers. The gateway is a low-cost VPN appliance that provides functionality, such as tunneling, encryption, and firewall services, as an adjunct to existing routers.

Gateways can also be used to overlay VPN security in existing IP networks. When adding security in this way, one consideration is whether responsibility for routing and security management should be separate or mixed. Many organizations have chosen to separate the responsibilities for network routing and security. However, Lucent's gateway security architecture supports either approach, allowing both separate and combined security and routing functionality and management.

VPN Router and Gateway Solutions

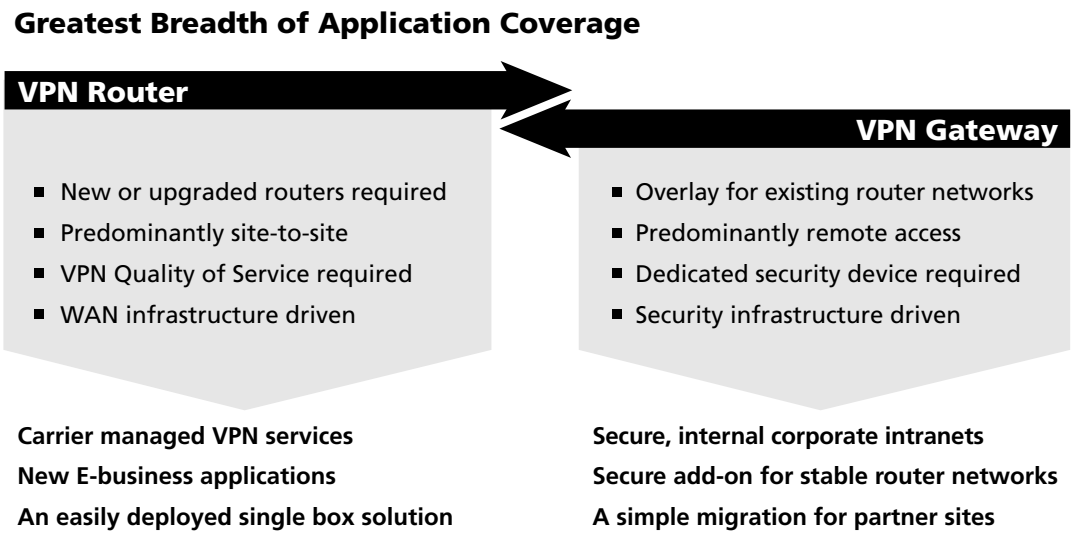


Figure 5

©2000 Lucent Technologies, Inc.

4. Lucent VPNWorX™ and Secure VPN Portfolio

The Lucent VPNWorX Portfolio

This suite of VPN products and management systems is the industry's most comprehensive framework for building VPN services. VPNWorX products fill every platform requirement from the carrier core to IPSec client software, VPN routers, and gateways. Centralized policy management caps the portfolio with extensible customer control and easy provisioning of robust service features. The VPNWorX portfolio breadth and depth allow optimal configurations with a choice of service platforms, security options, performance levels, management capabilities, and business models.

The Lucent Secure VPN Portfolio

Under Lucent's VPNWorX umbrella of enterprise-to-carrier VPN architecture solutions, the Lucent Secure VPN portfolio focuses on systems that are optimized for secure premises-based VPNs. The Secure VPN portfolio includes IPSec client software, VPN routers, and VPN firewall/gateways in one comprehensive package—all offering centralized policy management. This crucial feature delivers robust end-to-end security and performance management capabilities, designed from the ground up for granular customer control.

Enterprises may require products spanning the full Secure VPN portfolio to meet various needs. The portfolio breadth and depth allow optimal configurations, with a choice of service platforms, security options, performance levels, management capabilities, and business models—whether the VPN is DIY, outsourced, or a combination of both. This robust offering from Lucent Technologies sets a new standard for secure VPN service architecture.

Secure VPN Applications, Products, and Standards

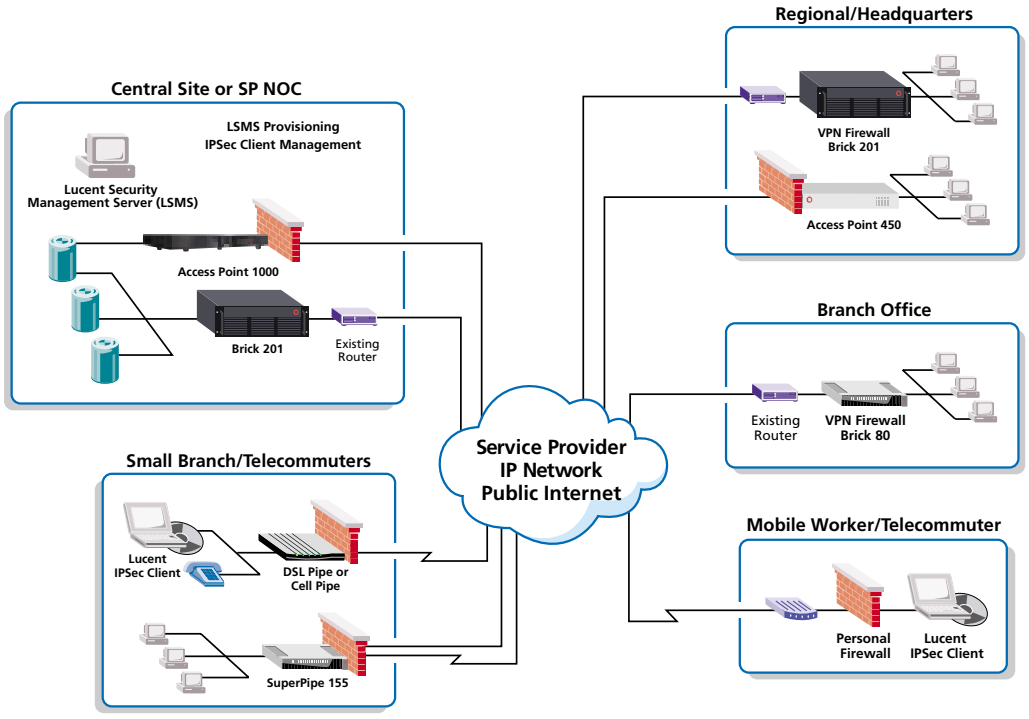


Figure 6 - Note: Each external location can represent an E-Commerce customer or supplier

©2000 Lucent Technologies, Inc.

Applications:

- **Site-to-Site Intranet:** Connections to 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 an enterprise network, VPNs allow corporations to take advantage of high-speed cable modem, satellite, and digital subscriber line (DSL) access.
- **Partner Extranet:** Quick setup and tear down of secure connections to extranet business partners, suppliers, customers, and government agencies.

Products:

- **Access Point™, SuperPipe™, and Pipeline® Routers:** Integrated VPN routers
- **Lucent VPN Firewall Brick:** Secure VPN Firewall and Gateway family
- **Lucent IPSec Client:** Integrated VPN client software
- **Lucent Security Management Server (LSMS) and QVPN Builder:** Centralized policy-based management

Security Standards:

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

Table 3

Lucent VPN Firewall Brick and IPSec Client

Priced starting at $4,000, Lucent VPN Firewall products provide IP networks with a cost-effective VPN overlay that includes robust firewall and hardware encryption services. Management is centralized and scalable to support thousands of IPSec software clients on mobile and remote user PCs. A highly secure ICSA and NSA-certified firewall is included in Lucent's VPN Firewall family, along with strong authentication and access control using best-of-breed, standards-based solutions.

The VPN Firewall Brick 201 is a purpose-built platform using hardware encryption to sustain 75 Mbps 3DES throughput, with up to 3,000 simultaneous tunnels. Nonencrypted throughput is 125 Mbps, with more than 100,000 simultaneous tunnels. Lucent VPN Firewalls use a proprietary operating system that eliminates standard operating system (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 works with any

©2000 Lucent Technologies, Inc.

LAN or WAN access solution (DSL, cable, ISDN or analog modem), giving telecommuters and mobile workers a choice of connections to an enterprise site.

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 device (router or firewall/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).

Access Point and Pipeline/SuperPipe VPN Routers

The Access Point and Pipeline/SuperPipe routers combine routing, bandwidth management, VPN, and firewall functions in integrated service platforms that have been purpose-built for industry-leading performance, price/performance, scalability, and ease of management. Deployed on-premises or at the service provider's PoP, these platforms serve both router and gateway functions for site-to-site or remote access applications of any scale.

Pipeline and SuperPipe Routers

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

Pipeline and SuperPipe routers combine integral WAN access, routing, IPSec tunneling and encryption, robust authentication services, and an integrated ICSA-certified firewall. The SecureConnect™ Firewall supports full dynamic IKE key management, PKI support (such as Entrust, RSA, and VeriSign), and user ID/password authentication using RADIUS and secure token options.

With centralized, automated VPN policy management through the 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 Routers

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 155 Mbps using DES or 3DES encryption.

Access Point routers also deliver IP QoS leadership with their class-based queuing (CBQ) technology. CBQ divides traffic into a hierarchy of classes, then assigns 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. The Access Point platform is fully DiffServ-compliant, achieving QoS signaling through the current IETF-defined industry standard.

Policy Management

At the core of the Lucent Secure VPN portfolio is an integrated, centralized VPN policy-management platform, the Lucent Security Management Server. The LSMS interfaces with RADIUS and SecurID user-authentication servers, and handles PKI and CA management of X.509 digital certificates. LSMS provides extensive auditing, logging, and alarm capabilities, and is integrated with a best-in-class intrusion detection system for enhanced security.

©2000 Lucent Technologies, Inc.

LSMS and QVPN Builder™

LSMS has proven itself as a centralized provisioning tool for enterprises and service providers that are building large-scale remote access. 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 optimized specifically for site-to-site provisioning of enterprise VPNs. With distributed but 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.

5. MAP-VPN Partner Solutions

Four Major Technology Categories

Four types of third-party application and infrastructure products have been integrated with Lucent's Secure VPN portfolio:

Content Security: Server-based software that provides network-level content filtering for anti-virus scanning and URL blocking to and from undesirable Internet sites.

High Availability: A combination of server-based software and hardware-based solutions that provide failover protection for the LSMS and firewall appliances respectively.

Authentication: Server-based software that provides crucial security features, including:

- Intrusion detection—the detection of and reaction to unauthorized access attempts from both within and outside the enterprise
- More robust access security via token password cards
- X.509 digital certificates/authorities for a higher level of security when using IPSec for tunneling

Infrastructure: Various products that simplify and enable more robust VPN access and management, including:

- Lucent's IPSec Client software
- Third-party IPSec client software from IRE that can support selected Lucent VPN products in lieu of, or in addition to, Lucent's own IPSec Client
- Sun Microsystems integrated UNIX* VPN workstations
- Third-party server-based reporting software that provides security management reporting in lieu of, or in addition to, the reporting capabilities inherent in Lucent's VPN products

Unique Internet Service Provider VPN Access Solutions

Lucent's VPN Firewall and IPSec Client are interoperable with both the GRIC and iPASS remote access dial-up solutions. The GRIC and iPASS dialers assure worldwide connectivity over the Internet. Once that connection has been established, users can seamlessly launch the Lucent IPSec Client, providing a secure, worldwide dial-up capability.

**UNIX is a registered trademark of The Open Group in the U.S. and other countries*

©2000 Lucent Technologies, Inc.

MAP-VPN Partners and What They Provide

Category	Partner	Product/Function
Technology Partners	1. ISS	Intrusion Detection
	2. VERITAS	Failover software for LSMS
	3. RADWARE	Failover hardware for the Brick
	4. Entrust	Digital Certificate AuthorityCA
	5. RSA	Token password cards and CA
	6. Trend Micro	VirusScan content filter
	7. Log-On Data	X-Stop URL blocking content filter
	8. Sun Microsystems	UNIXwork stations
Professional Services Partners	1. Teleias, Toronto	Integration, monitoring, and remote management
	2. Baker Comm, Dublin	Integration, monitoring, and remote management
	3. Zenfinity, NJ & India	Integration, monitoring, and remote management
Internet Service Providers Communications	1. UUNET	Outsourcing and managed services
	2. GRIC	VPN dialer bundle
	3. iPASS	Management services and VPN dialer bundle

Table 4

©2000 Lucent Technologies, Inc.

MAP-VPN Partner Fit

As shown in Figure 7, a ★ indicates where a MAP-VPN partner product can be incorporated in this sample Lucent solution. Sun products are easily integrated throughout.

MAP-VPN Partner Products in a VPN Solution

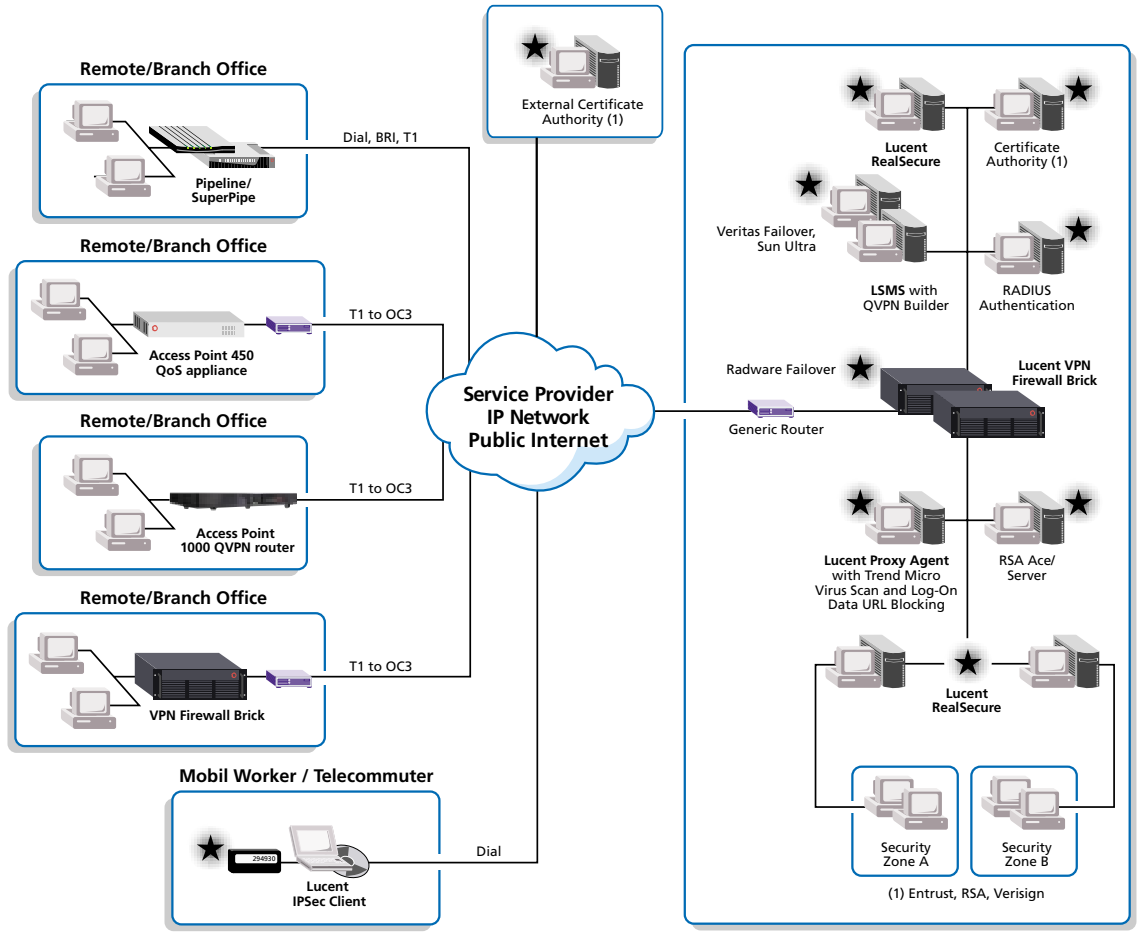


Figure 7

©2000 Lucent Technologies, Inc.

MAP-VPN Technology Partner Integration

Content Security

Trend Micro's InterScan* VirusWall is fully interoperable with the Lucent VPN Firewall/solution, where it resides on the Lucent Proxy Agent Server. InterScan VirusWall provides high-performance, three-in-one, real-time Internet gateway protection against viruses in SMTP, HTTP, and FTP traffic, and is the first enterprise-class virus protection product to incorporate detection of potentially harmful ActiveX** and Java*** code. InterScan VirusWall goes beyond pattern-based virus scanning, using its patented MacroTrap**** technology to detect known and unknown macro viruses. All routine tasks—scanning, updating, alerting, and reporting—can be automated and scheduled for maximum convenience and efficiency.

Integration with the Lucent VPNFirewall enables the customer to achieve a seamless, best-of-breed security solution. The Lucent VPN Firewall sends SMTP and HTTP network traffic through the Lucent Proxy Agent to InterScan VirusWall. Scanned traffic is then returned to the proxy, sent back to the firewall, and routed to its destination.

Interscan VirusWall and the Lucent VPN Firewall

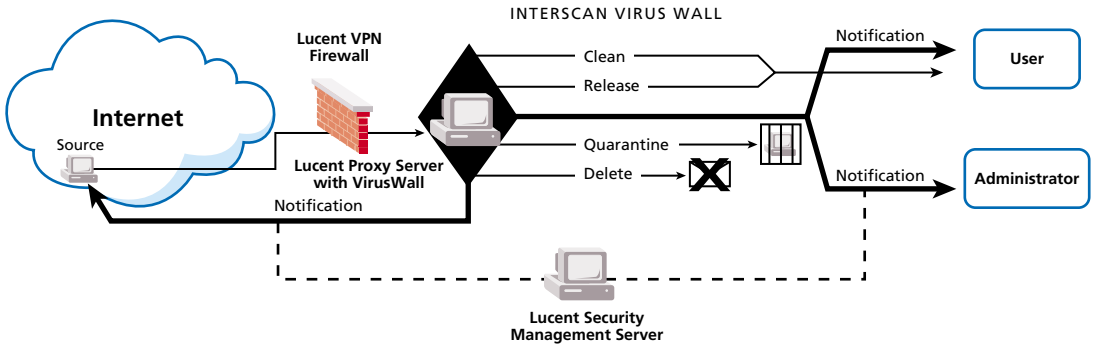


Figure 8

** InterScan is a registered trademark of Trend Micro, Inc.*
*** ActiveX is a registered trademark of Microsoft Corporation*
****Java is a registered trademark of Sun Microsystems*
*****MacroTrap is a registered trademark of Trend Micro, Inc.*

©2000 Lucent Technologies, Inc.

Log-On Data Corp. provides Internet content management solutions for businesses, schools, and ISPs. The company produces the industry-leading X-Stop* high-end Internet content-filtering software products that prevent access to sites with offensive content, such as pornography and promotion of hate crimes, while allowing access to educational and informational sites. X-Stop can also block offensive e-mail and time-wasting sites, such as gambling and online trading, which helps increase business productivity. The application is available for all types of networks including ISPs and large Internet backbones.

X-Server works in conjunction with Lucent VPN Firewall/Windows** NT and VPN solutions. Using the Lucent security software, X-Server provides Internet content filtering for HTTP, NNTP, and FTP traffic. It offers the most comprehensive filtering available, including Web site blocking, daily library updates, and a search engine monitor. These capabilities are based on an industry-leading library of blocked pornographic Web sites, along with more than 30 additional categories to be filtered.

The integration of X-Servers with the Lucent VPN Firewall provides a comprehensive, unsurpassed filtering solution. The Lucent VPN Firewall sends HTTP network traffic through the Lucent Proxy Agent to X-Server. Scanned traffic is then returned to the proxy, sent back to the firewall, and routed to its destination.

X-Servers Integrated with the Lucent VPN Firewall

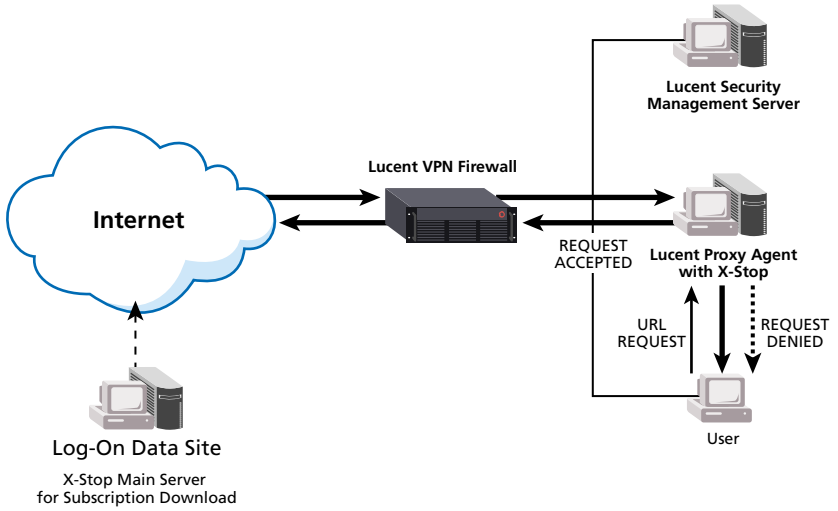


Figure 9

** X-Stop is a registered trademark of Log-On Data Corporation*
*** Windows is a registered trademark of Microsoft Corporation*

©2000 Lucent Technologies, Inc.

High Availability

RADWARE's FireProof* system provides the Lucent VPN Firewall with load balancing and failover capabilities for improved performance and availability. FireProof is a dynamic load-balancing system that intelligently distributes traffic between multiple firewall devices. It uses

an advanced array of built-in load-balancing algorithms to monitor the load on each firewall, directing traffic to the firewall best able to handle the user request. The FireProof system provides fault tolerance between firewalls in the case of a unit failure, and ensures uninterrupted service during periods of maintenance by redirecting all requests to an alternative firewall. The system's scalability allows additional firewalls to be incorporated and managed dynamically, in real time, transparent to the user community.

The integration of the FireProof load-balancing system with the Lucent VPN Firewall provides optimal performance, availability, and security. Inbound and outbound session requests are sent first through the FireProof system and entered into its client table. The request is then sent to the least busy firewall. With the FireProof system in place, session requests are guaranteed to travel through the appropriate firewall, maximizing availability and security.

FireProof System Integrated with the Lucent VPN Firewall

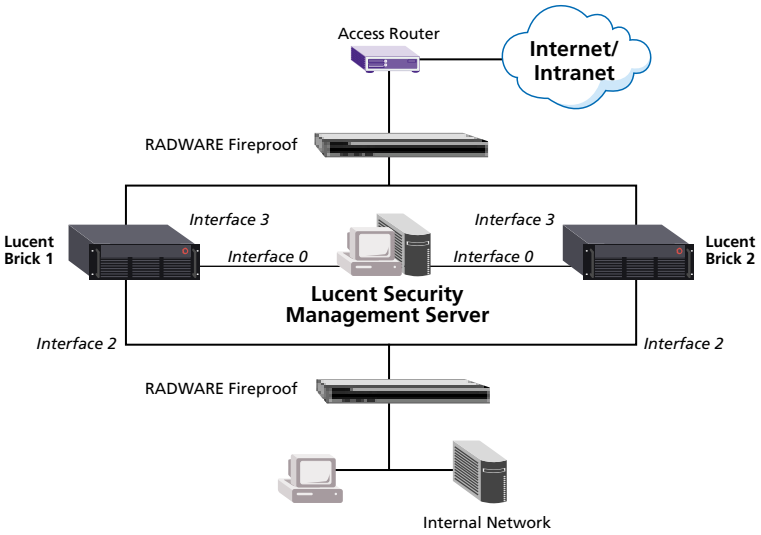


Figure 10

**FireProof is a trademark of RADWARE Ltd.*

©2000 Lucent Technologies, Inc.

VERITAS Software is the de-facto standard for application storage management, with more than 60 of the world's leading servers and operating systems integrating its software. These products provide continuous availability of business-critical information for companies of all sizes from some of the world's best-known blue-chip corporations to business managers to IT professionals. VERITAS Software is a premier strategic partner with all major industry drivers. The company's OEM customers and strategic alliances include industry pacesetters offering products at the device level to high-end UNIX vendors.

The integration of the VERITAS FirstWatch* platform with the Lucent VPN Firewall enables the deployment of highly available firewalls with no single point of failure. FirstWatch provides simple, yet robust failover management for Lucent Security Management Servers. Fault detection, isolation, and recovery are fully automated for the rapid restoration of services in the event of a failure. An entire node—or selected application services, configured into logical service groups—can be failed over to a backup node. Because it is non-intrusive, FirstWatch works with standard hardware and software components. Customizable, easy to install and manage, and flexible, it is an integral component in the management of highly available enterprise computing environments.

FirstWatch Integrated with the Lucent VPN Firewall

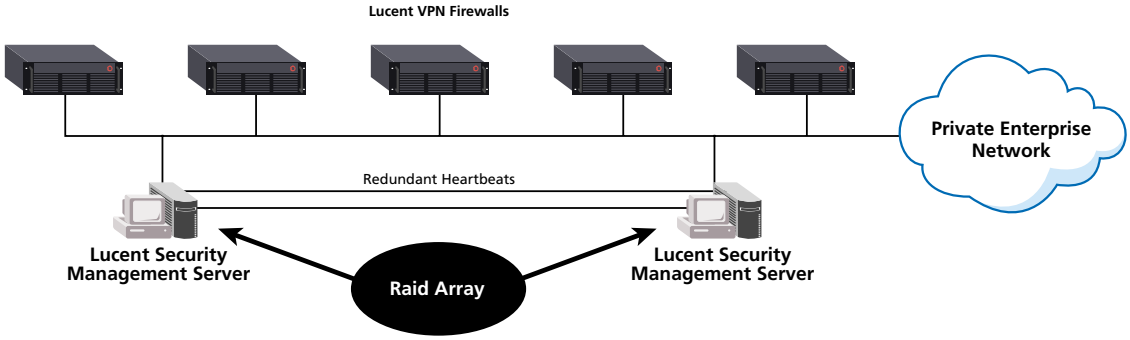


Figure 11

**FirstWatch is a registered trademark of VERITAS Software.*

©2000 Lucent Technologies, Inc.

Authentication

Internet Security Systems's (ISS) RealSecure* is the industry's first integrated host- and network-based intrusion, misuse, and response system. It unobtrusively analyzes network traffic and recognizes hostile activity by interpreting network traffic patterns that indicate attacks. RealSecure can also reside on individual hosts, reviewing system logs for evidence of unauthorized activity. Upon recognizing a threat, RealSecure responds immediately with a wide range of possible responses—from automatically terminating the connection to sending off alarms or pagers and recording the attack for forensic analysis.

RealSecure External and Internal Attack Protection

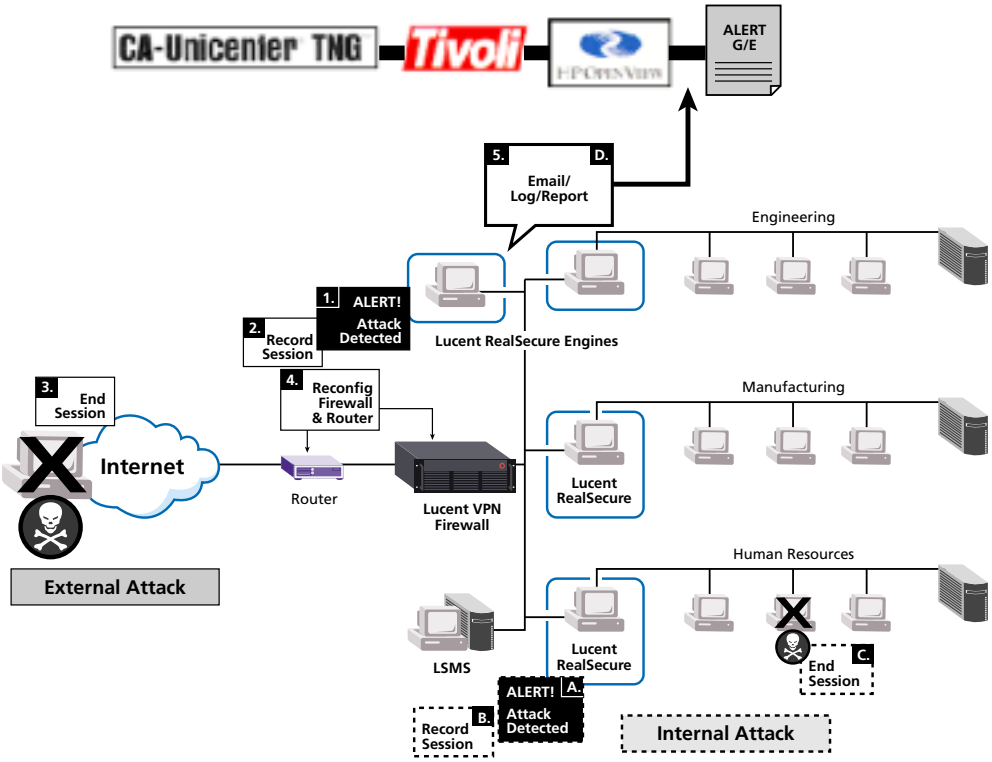


Figure 12

**RealSecure is a registered trademark of Internet Security Systems.*

©2000 Lucent Technologies, Inc.

The RSA SecurID* solution is at the heart of RSA's integration with the Lucent VPN Firewall. To provide security that far surpasses easily guessed passwords, RSA SecurID combines something the user knows—a PIN number—with something the user has—an authenticator device—much like an ATM card. RSA SecureID, authenticators generate unique access codes every 60 seconds. When combined with a unique PIN, the entire access code makes a user's identity immune to hacking, interception, or reverse engineering. The RSA ACE/Server verifies the authenticity of each user, based on time-synchronous authentication. RSA SecurID can also be utilized to secure the digital credentials of end users when using PKI-based solutions.

RSA's Keon** 5.0 PKI products enable, manage, and simplify the use of digital certificates in today's leading Internet applications. Whether deployed as a robust certificate authority or a complete PKI solution, RSA Keon is designed to secure e-Business and bring trust to today's new online economy. The Lucent VPN Firewall allows users to utilize RSA's standards-based digital credentials to ensure secure e-transactions over a VPN.

RSA Product Family

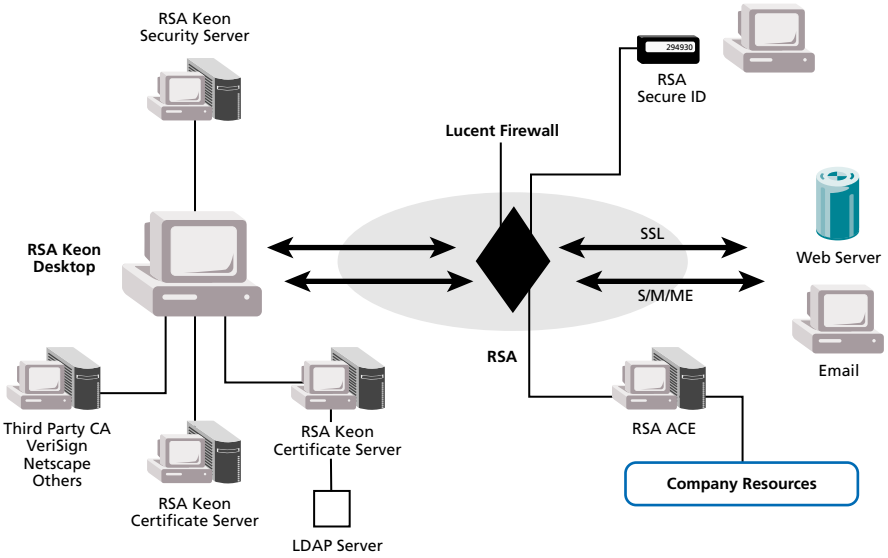


Figure 13

**SecurID is a registered trademark of Security Dynamics Technologies, Inc.*
***Keon is a tredemark of Security Dynamics Technologies, Inc.*

©2000 Lucent Technologies, Inc.

Entrust and Lucent have tightly integrated their technologies to create a comprehensive, scalable, easy-to-manage VPN solution. The Entrust/PKI software enhances the Lucent solutions by enabling certificate-based authentication for IKE VPNs. Entrust PKI Networking* manages the generation, signing, and revocation of X.509 certificates, and performs transparent key and certificate management for end users, which are all crucial for trustworthy global VPNs. Certificate-based VPN solutions leverage the scalable authentication capabilities of the Entrust/PKI. Using PKI within a VPN provides the following benefits:

- **Transparent, managed security that is easy to administer and use:** PKI hides the complexities of security from users with key and certificate management that is automatic and transparent. It allows single sign-on for all applications, including the operating system.
- **Scalability that supports millions of users:** Entrust/PKI software scales to the level required through high-capacity, high-availability, advanced-network bandwidth management, minimizing deployment costs.
- **Reduced administration:** Entrust/AutoRA integration with VPN products increases security while decreasing administrative time and effort. End users can simply prove their identity with wallet or HR information, over the Web or intranet, and complete certificate enrollment without messy cut and paste. No administrator assistance is required.
- **Flexibility that fits:** Centrally defined policy can be automatically enforced across all applications. Enterprises simply choose the CA, Registration Authority (RA), and end-user security policies that fit their organizations' policies and procedures.
- **Security with independent certification:** Entrust/PKI has been certified by the U.S. Government (FIPS 140-1), as well as international agencies (Common Criteria EAL-3).

Certificate-Based Authentication

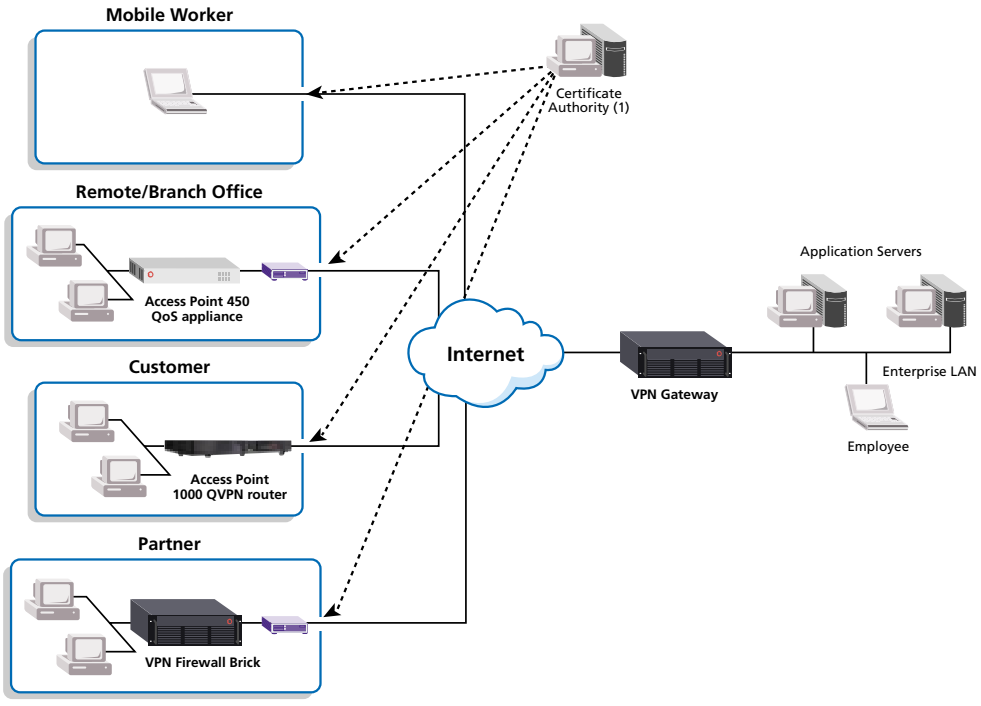


Figure 14

**PKI Networking is a trademark of Entrust Technologies, Inc.*

©2000 Lucent Technologies, Inc.

Infrastructure

Lucent and Sun

As shown in Figure 7, Sun workstations are used throughout the Lucent Secure VPN solution. Not only are Lucent application products running on Sun (that is, the LSMS) but most of the MAP-VPN partner products rely on Sun, as well.

About the SunTone Program

The SunTone Certification and Branding program is one of the industry's first collaborative efforts to define and audit service provider infrastructure, operational practices, hardware, software, and ultimately, overall service delivery—with the goal of providing quality levels of performance, security, availability, and uptime. The LSMS software is SunTone-certified to operate on Solaris platforms. The choice of Sun platforms is based on the network's unique requirements, such as the number of firewall and VPN rules that must be processed, the traffic load, and the number of Lucent VPN Firewall Bricks to be managed. Typical platforms for VPN solutions include:

The Sun Enterprise Ultra 10S server

- 440-MHz UltraSPARC -IIi processor supporting up to one GB of memory.
- Four PCI expansion slots, and up to 18.2 GB of internal storage. This system provides an excellent low-cost platform for business-critical network services.
- Up to four-GB of main memory, up to 364 GB of fast hot-swap Ultra SCSI internal storage, and over six TB of external storage capacity.

The Sun Enterprise 250 server

- Up to two 300- or 400-MHz UltraSPARC-II processors for extra-high performance.
- Six hot-plug Ultra SCSI disks and Fast Ethernet combine for unbeatable throughput.
- Sophisticated RAS features, including multiple independent data paths, ECC memory and data-path protection, automatic system recovery, built-in service processor with remote system control (RSC), and redundant hot-swap power.

The Sun Enterprise 450 server

- Up to four UltraSPARC-II processors—300-MHz or 400-MHz .
- 400-MHz UltraSPARC-II, with 4-MB Ecache memory and 360-GB internal storage.
- Six separate PCI buses providing more than 1-GB/sec I/O throughput.
- 32X SCSI CD-ROM.
- Two hot-swap 560W power supplies standard (three possible).

©2000 Lucent Technologies, Inc.

Internet Service Provider—Infrastructure Solutions Integration

GRIC is able to offer worldwide access to the Internet through the network of ISPs and Telcos that make up the GRIC Alliance Network*. GRIC Alliance members must install the GRICtraveler** client/server software to support worldwide Internet access (also known as global Internet roaming) for their users. The GRICtraveler software provides the authentication, authorization, and accounting functions needed to allow end users to get authenticated on the GRIC network, access the Internet, and track each transaction. GRIC settles all transactions among GRIC Alliance members.

Combining the GRICtraveler worldwide Internet access solution with Lucent's VPN Firewall and IPSec Client creates a complete, secure remote-access solution that meets the needs of ISPs and corporate enterprises alike. GRICtraveler works seamlessly with Lucent's VPN Firewall and IPSec Client to offer a secure, proven, and cost-effective remote VPN solution. The GRICtraveler/Lucent VPN solution is easy to use. The Lucent IPSec Client can be seamlessly launched, once the user has established an Internet connection using the GRICtraveler client software (GRICdial***).

How GRIC and Lucent VPN Work Together

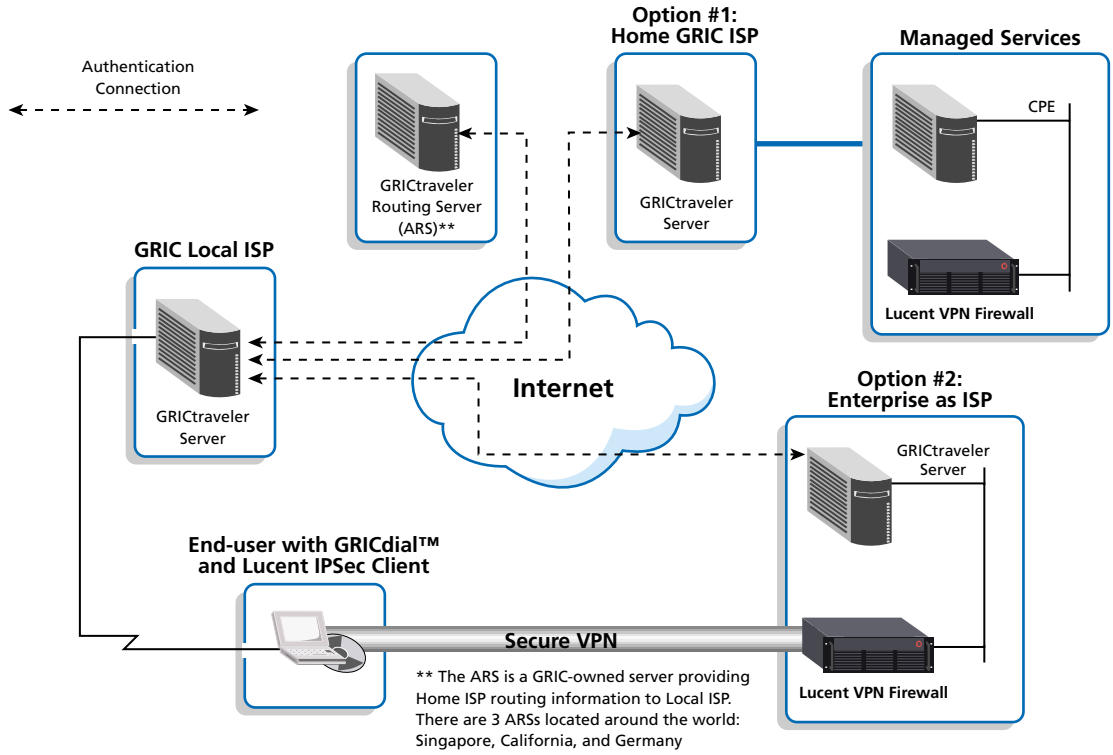


Figure 15

**GRIC Alliance Network is a trademark of GRIC Communications, Inc.*
***GRICtraveler is a trademark of GRIC Communications, Inc.*
****GRICdial is a trademark of GRIC Communications, Inc.*

©2000 Lucent Technologies, Inc.

iPass is a provider of remote access and internetworking settlement services that unlock the power of the Internet backbone for low-cost global communications. Through an alliance with the leading network providers around the world, iPass enables Internet service providers (ISPs), Internet carriers, and corporate customers to provide easy and secure Internet access with a local call through more than 5,000 access points in 150 countries.

iPass is the proven standard for global Internet roaming and corporate remote access/VPN solutions, and the company's settlement platform is used to enable other emerging Internet-based services. iPass provides high-value solutions to more than 700 Internet carriers and ISPs offering its global access services.

How iPass and Lucent VPN Work Together

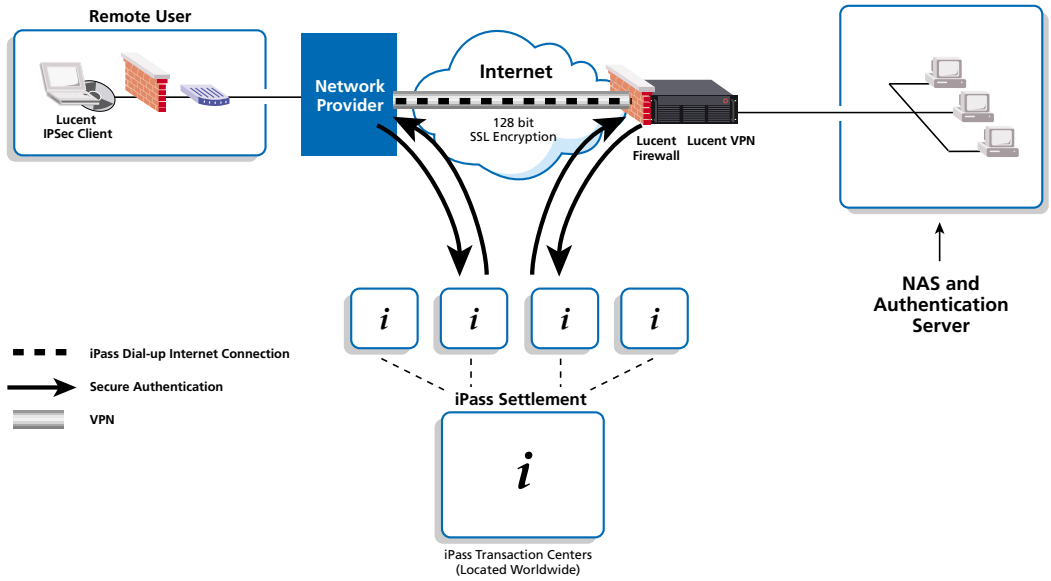


Figure 16

©2000 Lucent Technologies, Inc.

6. Conclusion

For both enterprises and service providers, VPNs are a fundamental solution for achieving global connectivity. Enterprises need to leverage their reach, becoming "virtual enterprises" with an extended community of partners, customers, and employees. Service providers need to expand their revenue-generating opportunities by providing effective and efficient managed services that assume responsibility for the communications network, protocols, and, if necessary, security.

Internal business drivers compel some organizations to build their own VPNs, while others outsource their solutions entirely or in part. With either approach, 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 example, to facilitate rapid deployment and global scalability, enterprises often choose to leverage service provider infrastructure, while still maintaining control over VPN access and security administration.

Further, service providers can take advantage of the growing realization among enterprises that deploying and managing VPN policy definitions across a myriad of VPN configurations can be too complex to handle effectively in-house. For small organizations, this process costs too much and distracts from core business. For large organizations, the scale can be so large, both geographically and technically, that outsourcing appears to be a superior alternative. However, if an enterprise cannot design its own policies for a service provider to implement, the VPN solution will remain DIY.

When choosing a VPN solution, it's important for both service providers and enterprises to consider a complete product line. These offerings should include 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 the ability to carve an IP network into unique customer-managed zones—are key enablers of VPN solutions. However, not all service platforms provide these capabilities. Lucent's industry-leading Secure VPN portfolio, combined with Lucent's MAP-VPN partners' industry-leading products and services, delivers the end-to-end dexterity and robustness required to build secure VPN solutions for any business need.

©2000 Lucent Technologies, Inc.