Secure Virtual Private Networks for Enterprise
February 1999

Secure VPNs for Enterprise Networks

This document provides an overview of Virtual Private Network (VPN) concepts using the Lucent VPN Gateway. Benefits of using VPNs and potential application scenarios are also discussed.

This document assumes that the reader possesses a basic understanding of Internet Protocol (IP) networking technology and encryption concepts.

Why Secure VPNs?

A secure enterprise VPN is often defined as "a network that uses encryption and authentication to build secure private tunnels over public networks." While the use of public networks and encryption technology to virtually create private networks is not a new concept – the U.S. military has applied it for years – it has not traditionally been applied by non-military organizations such as commercial enterprises. With the advent of IP security standards and the ubiquitous deployment of IP networks, VPNs are now feasible, even superior, alternatives for most enterprises.

Traditionally, enterprises created their own private networks by using private telecommunication circuits or networks. Unfortunately, these circuits (e.g., T-1 circuits) are expensive and often cannot be provisioned quickly, taking days or weeks to be put in place. For secure remote access, most enterprises have deployed their own dial-up remote access servers. These dial-up services require long distance or toll-free phone charges for non-local access, which can be quite expensive. Furthermore, maintaining your own remote access service requires complicated and expensive technology updates, as modem technologies improve and new access methods (e.g., DSL) become available.

Specific Benefits of Secure VPNs

Secure VPNs provide an excellent alternative to private, dedicated circuits and dial-up remote access servers. Secure VPNs can deliver many benefits to the enterprise:

- ***Cost savings*** – an enterprise can reduce costs on several fronts: the costs of leasing dedicated circuits or private networks, the costs of buying and maintaining remote access equipment, and the staffing costs of operating remote access services.

- ***Increased speed of service deployment*** – instead of waiting days or weeks to install new circuit connections, Secure/VPNs can be created in just minutes.

- ***Reduced exposure to changing technology*** – enterprises no longer need to worry about costly technology turnover (e.g., changing modem technology)

Private Communications Over Shared IP Networks

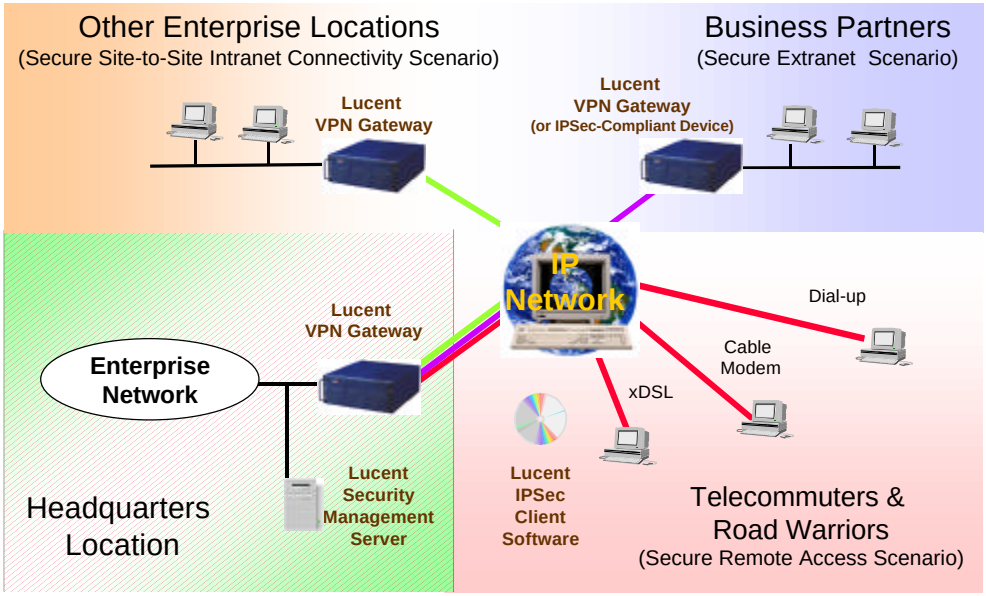
Virtual Private Networks allow the enterprise to leverage inexpensive and ubiquitous IP networks to perform critical enterprise services such as:

- ***Secure Remote Access***, more than just analog or ISDN dial-access to your enterprise network, you can also take advantage of high speed cable modem, satellite, and digital subscriber line (DSL) access

- ***Site-to-Site Connectivity***, connecting together various enterprise locations, such as branch offices and headquarters locations, using low cost IP networks instead of dedicated circuits or frame relay networks.

- ***Secure Extranets***, allowing quick setup and teardown of secure connections to "extranet" partners – business partners, suppliers, customers, government agencies.

The network diagram below illustrates the application of the Lucent VPN Gateway to these scenarios.



Lucent VPN Gateway Applications

The Lucent VPN Gateway has been designed in accordance with the IPSec protocol for Virtual Private Networking over the Internet. This enables the Lucent VPN Gateway to securely communicate with other IPSec-compliant devices. For more information on the IPSec protocol, see the "Frequently Asked Questions" section of this document.

The Lucent VPN Gateway provides a strategic alternative to existing technologies in securely supporting these remote access, site-to-site intranet, and extranet applications. The table below lists the pros and cons of each alternative.

Application	*Typical Methods*	*Strategic Alternatives*
Secure Remote Access	**Dedicated Remote Access Servers** • Access technology is expensive to operate • Incurs high telephone charges for non-local access • Requires frequent modem pool upgrades (14.4k → 28.8k → 33.6k → 56k → ??)	**Lucent Secure VPNs** • Leverages low cost IP networks • "Outsources" operation of access technology to skilled providers (ISPs, Cable companies, DSL providers) • Eliminates long distance charges • Avoids expensive modem technology upgrades
Site-to-Site Connectivity	**Dedicated Links or Frame Relay Networks** • More expensive than Internet access • Takes time to procure • Centralized Internet access forces Internet-bound traffic back over internal networks to central gateway	**Lucent Secure VPNs** • Leverages low cost IP networks • Reduces traffic on internal site-to-site network by allowing each site to directly access Internet in accordance with security policy

	Dedicated Links (e.g., 56k, T1)	Lucent Secure VPNs
Secure Extranets (External Network Connections)	• Expensive • Takes time to procure • Usually requires dedicated port on firewall to adequately secure	• Leverages low cost IP networks • Can be set up or torn down rapidly with almost no marginal cost • Can be secured with an individual security policy (a "virtual" firewall) • Standards-based for interoperability with other vendor's equipment

Application of Secure VPNs Compared with Traditional Options

Secure VPN Application Scenarios

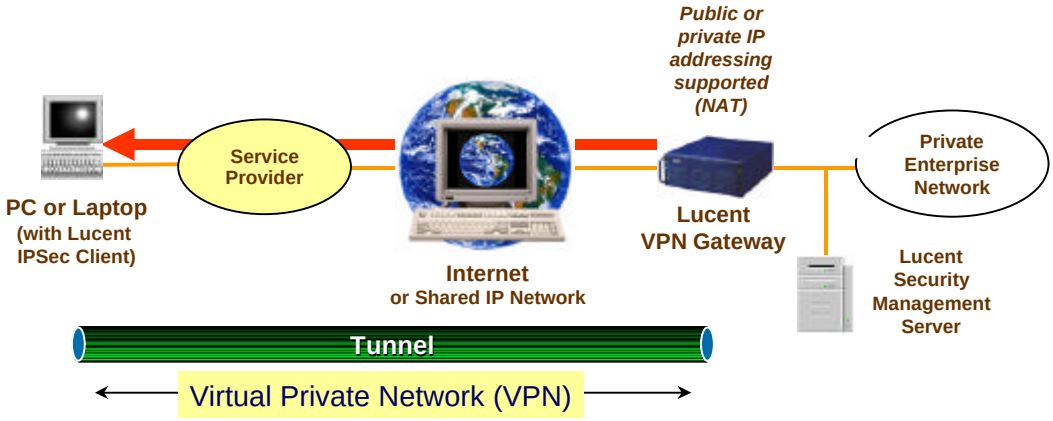
The Lucent VPN Gateway supports a variety of application scenarios. Three common scenarios are described below, including secure remote access, secure site-to-site Intranet, and secure Extranet scenarios.

Secure Remote Access Scenario

In our first application scenario, we consider an enterprise that has a traveling sales force or traveling executives (i.e., road warriors) and telecommuters that need to access the enterprise network.

Example remote access applications might include:

- ***E-mail,*** using SMTP, POP-3, IMAP-4, or e-mail packages such as Microsoft Exchange™ or Lotus Notes™
- ***Web,*** access to enterprise Intranet HTML and JAVA applications
- ***File Access,*** via FTP or using Microsoft Networking protocols (to allow for file browsing using Microsoft Windows™ Explorer)
- ***Database,*** a database application possibly with a Web front end
- ***Telephony,*** voice over IP



Secure Remote Access Configuration

In this secure remote access environment, depicted above, the telecommuter or road warrior with a Microsoft Windows™ PC or laptop can connect to a global or local IP service provider for IP connectivity to the Internet or other shared IP network. In the case of dial-up connectivity, a PPP connection is usually established between the Windows™ PC and the service provider, where the provider issues a dynamic IP address. In the case of other connection methods (such as cable modem or DSL), addresses are also assigned by the service provider. Sometimes the assignment is dynamic and sometimes it is static. In either case, the type of access method does not affect Lucent's VPN application. Popular access methods that are compatible with the Lucent VPN Gateway include:

- ***Analog Dial-up***
- ***ISDN***
- ***Cable Modem***
- ***Digital Subscriber Line (DSL)***
- ***Satellite Access***
- ***Ethernet***

Once connected by the applicable access media, the remote access user can connect securely to the enterprise network by simply "enabling" a Secure VPN using Lucent's IPSec Client software. This is done via our easy-to-use graphical user interface (GUI). The Lucent IPSec client then connects to the Lucent VPN Gateway. The VPN Gateway automatically and transparently authenticates the user and downloads a security policy database to the Lucent IPSec Client software. The security policy database dictates what connections are permitted, which ones should be encrypted and sent via the VPN Gateway, and which ones should be passed in the clear without encryption or without being sent via the VPN Gateway.

Site-to-Site Intranet Connectivity

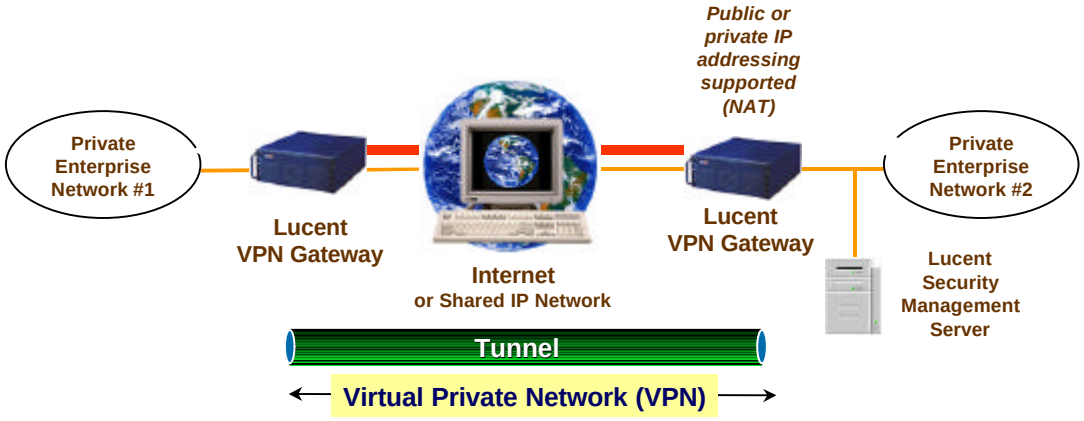
In our second application scenario, we consider an enterprise that has multiple locations and wants to connect those locations together. This has historically been accomplished using point-to-point links or "private" frame relay networks. In such a configuration, all Internet-bound traffic must traverse the internal private network to reach the nearest Internet gateway.

By using shared IP networks (or the Internet) instead of point-to-point links, Internet-bound traffic can exit each location via its own Internet connection. Of course, an enterprise can still force all traffic to be routed via specific Internet gateways (at the headquarters location, for example). The enterprise can use the shared IP network as a private backbone by tunneling all private IP traffic through an IPSec tunnel from one VPN Gateway to another. These features give the enterprise tremendous flexibility in managing network traffic flow.

Example site-to-site Intranet connectivity remote access applications might include:

- ***E-mail,*** both client-to-server e-mail access and mail gateway-to-mail gateway e-mail exchange.
- ***Web,*** access to enterprise Intranet HTML and JAVA applications
- ***File Access,*** via FTP or using Microsoft Networking protocols (to allow for file browsing using Microsoft Windows ™ Explorer)
- ***Database,*** database access or database-to-database transfers
- ***Telephony***, voice over IP
- ***Video conferencing***
- ***Multimedia applications***
- ***Other Enterprise IP services***

In the diagram below, the Site-to-Site VPN is depicted. As shown, the secure IPSec tunnel extends between each Lucent VPN Gateway. Traffic originating from one of the enterprise's networks destined for another travels through this secure IPSec tunnel, however this is completely transparent to the sender and the recipient. No special software or configuration is required for the sender or recipient.



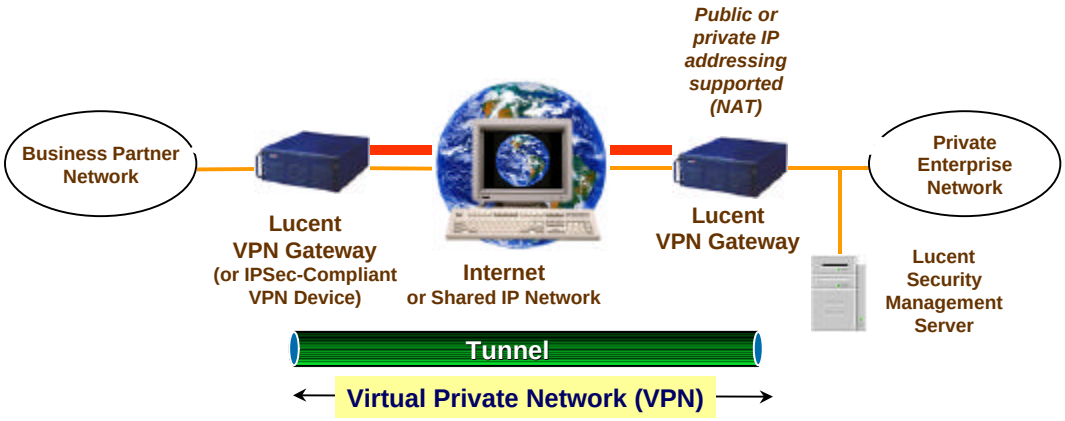
Secure Site-to-Site Intranet Configuration

In the above example, security can be applied based on the VPN Gateway's security policy. For example, if traffic between two specific hosts is extremely sensitive, Triple DES can be applied to that traffic. If traffic between two other hosts is not sensitive, DES can be applied, or (if the organization's security policy permits), packet authentication can be applied without encryption. This is all under control of the administrator.

Secure Extranet Connectivity

In our third application scenario, we consider an enterprise that has multiple "extranet" partners, such as business partners, joint venture participants, suppliers, or customers. Typically, these connections are served today by point-to-point links (e.g., T-1s) that take a long time to procure and are expensive to operate. By using an existing IP network connection, a VPN can be set up with an extranet partner in a matter of minutes. By using an existing IP connection, the marginal cost of adding the extranet partner can be minimized.

These connections typically support a fairly limited set of services that are often driven by the business needs of the relationship between the two organizations. For example, one relationship may require sharing of a SQL database, while another relationship may require only web access to specific web servers. By using the Lucent VPN Gateway, with its embedded ICSA-certified firewall, you can secure your extranet connections in a more robust and easily-managed fashion. The VPN Gateway's "Security Zone" feature allows a separate and separately managed security policy to be set up for each extranet partnership. Each extranet security policy can be contained in a separate Security Zone – no mixing of rules for different connections is required.



Secure Extranet Configuration

In the above diagram, a secure Extranet VPN is depicted. As shown, the secure IPSec tunnel extends between each Lucent VPN Gateway. Traffic originating from the enterprise's network destined for a business partner travels through this secure IPSec tunnel, however this is completely transparent to the sender and the recipient. No special software or configuration is required for the sender or recipient. In fact, the business partner does not need to have a Lucent VPN Gateway – the business partner can use any IPSec-compliant VPN device.

What to Look for in a VPN Solution

When considering a VPN solution, it is important to look beyond the data sheet technical parameters to also consider several higher level requirements. By considering these areas before making a procurement decision, you are more likely to end up with a solution that meets your needs, both today, and as your network evolves in the future.

- ***Strong Security*** – your VPN solution is just as critical as your firewall, as VPNs are "security perimeter" devices that separate your internal network from the outside world. Look for a *real* ICSA-certified firewall – not some "firewall filters" or "access control lists" that may have been added as an after-thought. Avoid using general-purpose operating systems as a foundation for your VPN devices, as they can be full of security holes.

- ***Standards Compliance*** – *the* standard for secure VPNs is IPSec, an IETF standard. Don't be fooled with proprietary security technology or with a "we're transitioning our security to IPSec" promise.

- ***Ability to Grow*** – most enterprises experience growing or changing networking needs (e.g., faster connections, more locations). The ability to grow your VPN solution without wholesale hardware/software replacement is important.

- ***Hardware Encryption Acceleration*** – the processing required to perform encryption and decryption is intensive, particularly for performing automated key exchange. Software-only solutions generally provide limited performance.

- ***Integrated Security Management*** – your VPN is a critical part of your security infrastructure. Look for vendors that allow you to manage your VPNs in tight synchronization with your firewall and intrusion detection.

- ***A Trusted Networking Vendor*** – look for a reliable networking solutions provider that will stand behind their products and will be there to help you as your needs change.

Frequently Asked Questions

The subject of VPNs is a complicated one. There are many questions that often arise when considering VPN deployment. Some of the most common questions are listed below.

What is IPSec?

IPSec is the Internet Engineering Task Force's (IETF) Internet Protocol (IP) Security (IPSec) standard. It is composed of a collection of Internet RFCs that address the confidentiality, integrity, authentication, and access control of IP packets. It is *the* standard for IP security. The collection includes standards for encryption and authentication, as well as standards for key exchange. This standard was developed by the IETF's IP Security Protocol Working Group, of which Lucent is an active participant. For more information on the standards, please see the following RFCs:

- Security Architecture for the Internet Protocol (RFC 2401)
- IP Authentication Header (RFC 2402)
- The OAKLEY Key Determination Protocol (RFC 2412)
- IP Encapsulating Security Payload (ESP) (RFC 2406)
- Internet Security Association and Key Management Protocol (ISAKMP) (RFC 2408)
- The Internet Key Exchange (IKE) (RFC 2409)

For more information on the working group, see: http://www.ietf.org/html.charters/ipsec-charter.html

Is IPSec important, or can I go with one of those other protocols?

For network security, IPSec is the only standard. PPTP may not provide adequate security (several experts have questioned the security of PPTP and several PPTP implementations have contained security holes that have been exploited). L2TP relies upon IPSec for security. Proprietary security approaches may or may not be secure. The best choice for security is IPSec.

Can't I just add VPN software to my routers?

This depends on your networking environment. For a main-office (e.g., headquarters or medium/large-office location), a dedicated VPN device is recommended. VPNs require significant processing power, which can put a performance drag on your routers. It may not be advisable to use VPN software as an "add-on" to a router, as peak VPN connectivity could adversely affect router performance. However, for small-office, home-

office, or branch-office locations, where the number of VPN users is limited to a small number, software add-ons may be perfectly acceptable.

Another consideration is whether you want to mix organizational responsibility for security with routing. Many organizations have chosen to keep separate the responsibilities for network routing and for network security. Because both are topics unto themselves, many enterprises rely on separate pools of expertise for each. Lucent's security architecture allows for separate management of security and routing functions, if desired, or for combined management, as well.

Can't I just run some VPN software on a general-purpose operating system?

Running off-the-shelf VPN software on top of a general-purpose operating system introduces significant security concerns and performance limitations. The battle to keep general-purpose operating systems "secure" by applying the latest patches is a never-ending battle. Furthermore, these operating systems contain a huge amount of code that is unnecessary to the task of providing security, creating a performance burden and unknown security risks. Finally, the potential for subtle and often undetected misconfiguration of general-purpose operating systems makes them a bad foundation for security.

What about availability and reliability of the Internet?

While the Internet itself may not "accountable" to an enterprise and may not always provide adequate availability, an Internet service provider (ISP) can deliver IP network connectivity with high levels of availability and reliability. An ISP can provide service level agreements (SLAs) for their service, upon which reliable business services can be delivered. An enterprise can contract with one or more service providers to obtain a solid IP network foundation upon which highly reliable Secure/VPNs can be deployed.

For More Information

For more information on how to take advantage of the Lucent VPN Gateway's high level of security, scalability, and manageability, please visit the Lucent VPN Gateway web site at http://www.lucent.com/security or call +1 888 552-2544.