Your Short Cut to Knowledge

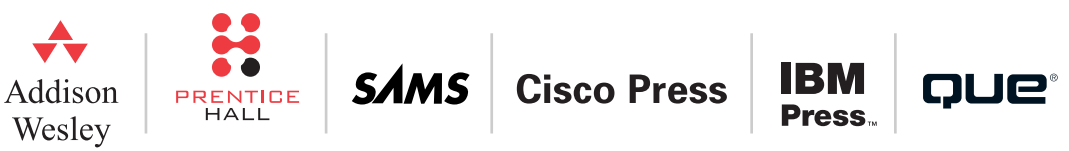
The following is an excerpt from a Short Cut published by one of the Pearson Education imprints.

Short Cuts are short, concise, PDF documents designed specifically for busy technical professionals like you.

We've provided this excerpt to help you review the product before you purchase. Please note, the hyperlinks contained within this excerpt have been deactivated.

Tap into learning—NOW!

Visit **www.informit.com/shortcuts** for a complete list of Short Cuts.



VPN Technology Primer and Comparison of VPN Technology Options

The main focus of this chapter is on VPN technology, protocols, and concepts. This chapter presents a comparison of multiprotocol label switching (MPLS), IP security (IPsec), and Secure Socket Layer (SSL) to give you a good understanding about the benefits and shortfalls of choosing each technology for a VPN solution. This is a standalone section that can be read without working through Chapter 1, "The VPN Technology Promise: Secure Access from Anywhere to Anything." Even though this chapter is more technical in nature, it is essential for managers and CIOs of organizations considering deployment of a VPN solution to review this material. The comparisons in this chapter help develop an appreciation for the design considerations, deployment challenges, and management of technology for a successful VPN solution implementation.

Choosing the Right VPN Solution—A Technology Primer

In this technology primer, three technologies are discussed with VPN deployment in mind, and a comparison is provided because the main focus of this Short Cut is making a decision about how to implement a VPN. You can learn specifics about the technology, protocols, and concepts in detail from several other Short Cuts after you've made your initial decisions. This chapter helps you compare key factors for the following three VPN technologies before you make your implementation decision:

- MPLS
- IPsec
- SSL

> **Note:** For a detailed look at MPLS-based VPNs, consider reading *MPLS and VPN Architectures,* by Ivan Pepelnjak and Jim Guichard.
>
> For a detailed look at IPsec VPNs, consider reading *IPSec VPN Design,* by Vijay Bollapragada, Mohamed Khalid, and Scott Wainner.

Indicators That MPLS Is a Good Choice

MPLS is essentially a label-switching technology and provides switching at Layer 2 in a time-efficient manner, making delivery of IP packets faster than normal IP routing at Layer 3. In addition, MPLS VPN provides the privacy and quality of service (QoS) of ATM and Frame Relay Layer 2 services, as well as the flexibility, scalability, and connectivity of IP. We can now combine them into a single service for the first time.

The reason we can do this is that MPLS is modeled on label-based forwarding at Layer 3. This essentially provides a foundation for IP value-added services.

MPLS VPNs provide the capability to flexibly group users and services into arbitrary groups with arbitrary services. This is an essential element and is a foundational change to prepare the network infrastructure to deliver IP services in a cost-effective and rapid manner.

Low-cost managed IP services delivery on MPLS VPNs are feasible because lower operational costs allow service providers to deliver private IP services to businesses with required management capabilities.

The following factors help enterprises to determine when to use MPLS:

- The company needs SLAs for network operation assurance.
- Security needs are met by traffic separation similar to that of Frame Relay or ATM.
- Traffic patterns are suited for a partial or full mesh topology.
- The enterprise plans to converge its data, video, and voice traffic onto a single network; therefore, delay-sensitive traffic, such as voice, video, or mission-critical data, must receive the necessary QoS.
- Implementation is very large or growing.
- The enterprise wants to deploy multicast applications.
- The enterprise wants to deploy additional value-added applications, such as multimedia conferencing, e-collaboration, or business-process applications such as order fulfillment, enterprise resource planning (ERP), or customer relationship management (CRM).
- The enterprise wants to outsource its WAN.

Note: The preceding factors for MPLS VPN are referenced from the following:

http://cisco.com/en/US/partner/netsol/ns465/networking_solutions_white_paper0900aecd801b1b0f.shtml

MPLS User Experience

As a network-based VPN service, MPLS does not require the use of a VPN client. Enterprise end users typically interact with the network as they would ordinarily.

For telecommuters and mobile workers, a virtual route-forwarding (VRF) instance may be assigned to the Remote Users Profile, and IP packets belonging to this VRF may be switched accordingly. If these telecommuters and mobile workers are traversing through a public Internet, they can use IPsec for secure transmission of IP packets. After terminating the IPsec tunnels on an aggregation point or head-end, which may be a provider edge (PE) router, all clear text traffic may be mapped into an instance of VRF that subsequently is label switched.

MPLS Strengths

The primary strengths of an MPLS-based VPN for the enterprise are the following:

- **Network security**—MPLS enforces traffic separation among different VPNs on the same core network by using route distinguishers. Unique route distinguishers are assigned automatically when the VPN is provisioned and is placed in packet headers.

MPLS VPN privacy is similar to the privacy in traditional WAN infrastructures such as Frame Relay and ATM, and its effectiveness has been demonstrated by Miercom, which provides independent testing and analysis of networking services. The service provider can design the network so that customer routers have no knowledge of the core network, and core routers have no knowledge of the customer edge.

- **Scalability**—A well-executed, MPLS-based VPN deployment scales easily to accommodate company growth or changes. It does not require the full-mesh, end-to-end peering that other VPN architectures require. For example, when a new site is added to the VPN, the company or service provider needs to establish local peering only between the new site and the provider edge. It does not need to reconfigure the CPE at other existing sites, gaining significant operational cost savings.
- **Support for SLAs**—SLAs are important to enterprises with stringent requirements for network performance and resiliency. MPLS-based VPNs support SLAs by providing scalable, robust QoS mechanisms, guaranteed bandwidth, and traffic-engineering capabilities. By deploying traffic engineering in the core network, service provider network engineers can implement policies to help ensure optimal traffic distribution and improve overall network usage.

When to Implement MPLS

Because MPLS VPN provides the foundation for IP services, it is essential to deploy when you anticipate using it to deploy future IP services. An example is IP telephony solutions. MPLS provides a great foundation to provide IP telephony—essential to business communication in a cost-effective manner.

Generally, when QoS and privacy without encryptions are warranted, MPLS VPNs are chosen.

MPLS VPN Considerations for Building Versus Buying

For businesses, moving to MPLS VPN is a technology shift. With WAN routers connecting to the Internet, businesses have to incur the cost of buying bandwidth. It is advisable to look for an MPLS bundle because to truly benefit from Internet connectivity and provide access to partners, a mobile sales force, and remote workers, it is becoming essential to deploy VPN VRFs directly on the WAN router.

Building MPLS VPNs is quite an undertaking for a business IT department. Adequately skilled staff for design, deployment, and rollout are essential to deploy VPN. As MPLS VPNs are getting commoditized, it is becoming more common for businesses to outsource MPLS VPNs that were built by the IT department at one stage. Again, for businesses, negotiations when procuring bandwidth purchase can help identify the bundle that allows service providers to manage the router freeing up the IT department and at the same time get the business technology ready so that other IP services can be deployed very rapidly.

Drawbacks of MPLS VPN

As the technology shift continues to happen in the marketplace, no real drawbacks exist for deploying an MPLS VPN. In terms of an IT department's skill levels, MPLS VPN requires more skilled staff that may be already in short supply because of mass deployment of the technology. In reality, the advantages of deploying an MPLS VPN far outweigh the drawbacks.

Indicators That IPsec Is a Good Choice

The main driver for IPsec deployment is the confidentiality gained because of encryption. Other tenants of CIAN that are essential when adhering to regulatory requirements become mandatory for businesses.

IPv4 by design has considerations that make it secure in operation. This goes back to the Internet changing from a "model of inherit trust" to a "model of pervasive distrust" with a history of attacks and malicious activities adversely affecting businesses connecting to the Internet. Businesses also wanting to secure their intellectual properties, especially in areas such as technology, biotech, and manufacturing, deploy IPsec to add to the privacy provided by MPLS VPN.

The following factors help enterprises to determine when to use IPsec:

- The enterprise needs security measures such as data encryption or user and device authentication. IPsec provides strong security beyond the traffic separation inherent to MPLS, Frame Relay, or ATM networks. Enterprises that choose the MPLS VPN architecture because of its scalability and QoS support sometimes augment it with IPsec when they need additional security functions such as data encryption.
- Cost considerations are important. An IPsec VPN can be deployed across any existing IP network, avoiding the capital and operational expense of building a new network.
- The enterprise needs to extend its corporate network resources to geographically dispersed teleworkers and mobile workers.
- Rapid deployment is important because the business can quickly add a new site or expand to a new location. IPsec saves time because it requires little or no change to the existing IP network infrastructure.
- Traffic flow follows a hub-and-spoke topology.

Note: The preceding factors for IPsec VPN are referenced from http://cisco.com/en/US/partner/netsol/ns465/networking_solutions_white_paper0900aecd801b1b0f.shtml

IPsec User Experience

The user experience for site-to-site and remote-access VPNs varies slightly.

Remote-Access User Experience

Typically, the user invokes the VPN software client and selects the appropriate destination, such as a hostname or IP address. After successful authentication and IPsec tunnel setup, users can access applications as they would from their offices. IPsec allows access to almost all networked applications, without modifications to the hosted site or client.

Site-to-Site User Experience

For site-to-site connectivity via an IPsec-based VPN, users do not need client software on their computers. Instead, the user at a branch office launches the application as if it resided locally. An IPsec-enabled VPN router at the branch office automatically initiates an IPsec session with the central office. Upon successful session negotiation and authentication, a secure VPN tunnel is established between the branch and central office, without any action by the user.

IPsec Strengths

The primary strengths of IPsec-based VPN for the enterprise are as follows:

- **Low cost**—Low-cost Internet access can be used for network transport.
- **Strong security**—Inherently strong security features enable user authentication, data confidentiality, and integrity. Users are authenticated with digital certificates or preshared keys. Packets that do not conform to the security policy are dropped.
- **Support for teleworkers and mobile workers**—Head-end IPsec VPN devices scale to serve many thousands of geographically dispersed users.
- **Ease of deployment**—No service provider intervention is required to set up the VPN, although many enterprises choose to take advantage of the service provider's managed-service experience for regional or national multisite deployments to reduce costs, accelerate service introduction, and mitigate risk.
- **Reduced congestion at hub site**—When configured for split tunneling, the remote VPN client can forward Internet-destined traffic directly, instead of through an IPsec tunnel, and establish a tunnel only for related traffic being forwarded to the hub. This reduces congestion at the hub site.

When to Implement IPsec

To achieve VPN connectivity, especially for remote access IPsec VPN, a remote client is required. Depending on the solution, a software VPN client is installed on the end station connecting to the IPsec VPN head-end, or a hardware client is deployed providing IPsec connectivity to multiple clients connected to the LAN. In turn, only a hardware VPN remote client needs to connect to the IPsec VPN head-end, and traffic

from all the end stations on the LAN is secured by IPsec VPN. Bearing that in mind, here are some of the reasons IPsec VPN would be the best solution to deploy:

- IPsec-based VPNs are application agnostic. This means that any application may be accessible from anywhere, given that adequate IPsec VPN access is provided. For example, advanced applications such as telephony or QoS will be able to function over IPsec tunnels.
- IPsec will allow access to almost all network applications without modifications to the central site or client.
- IPsec will allow almost all applications to be supported without custom changes.

As IPsec is designed for IP unicast traffic only, with adequate support for IP multicast over the virtual adapter concept, IPsec can provide an experience equivalent to that at an office.

IPsec VPN Considerations for Building Versus Buying

Designing, deploying, monitoring, and maintaining IPsec VPN is truly a complex task. Each stage requires highly skilled professionals to get the job done right. As a result, IPsec VPN deployment as a managed service has experienced enormous growth over the past few years. This growth continues as more and more businesses are opting to buy IPsec VPN service from their preferred service providers.

An important observation for midsize to large businesses with a skilled IT department is that after building an IPsec VPN solution with help from a system integration partner, monitoring and maintenance of the IPsec solution can be outsourced. This way, the IT department can regain focus on optimizing applications required for the business operations and success over the deployed IPsec VPN.

Drawbacks of IPsec VPN

The following is a list of drawbacks for an IPsec VPN solution:

- Remote clients participating in IPsec VPN need client software installed.
- For the remote hardware client, traffic from each end station to the remote hardware client still traverses LAN in clear text.
- As interesting traffic is encapsulated into an IPsec tunnel, efficiency of payload in the IP data packet is decreased because of IPsec protocol overheads.
- Designing, deploying, and troubleshooting an IPsec VPN is a complex task. You need highly skilled professionals with good operational experience.
- Because multivendor solutions are seldom deployed, interoperability among different vendors has not been proven in the marketplace, adding to the original complexity of the IPsec VPN solution.

- The most recommended and secure method for key exchange is IPsec client-based certificates. However, certificate distribution authorities themselves are a complex undertaking.
- Retaining QoS takes some design efforts in the IPsec VPN solutions because most crypto engines in the hardware devices found in the market today cannot prioritize high-priority traffic when encrypting or decrypting the traffic.
- With the ESP flavor of IPsec VPN, network address translation (NAT) and port address translation (PAT) present a huge problem as the authentication checksums fail because of change in the IP header address.

Indicators That SSL Is a Good Choice

SSL-based VPN is the newest of the three VPN technologies compared in this chapter. It provides remote access connectivity from almost any Internet-enabled location using a web browser and its native SSL encryption. Although application accessibility is constrained relative to IPsec VPNs, SSL-based VPNs allow for access to a growing set of common software applications. SSL-based VPNs require slight changes to user workflow because some applications are presented through a web browser interface, not through their native GUI. Client/server application support generally requires specific and sometimes browser-dependent applets to be dynamically downloaded to the remote system. Using web technology for connectivity allows accessibility from almost any Internet-connected system without needing to install additional desktop software. Because an SSL-based VPN can provide network access to users from almost any Internet-connected system, it is an emerging option for extending remote access to users who require access to specific applications.

The main role of SSL is to provide security for web traffic. SSL provides confidentiality by using cryptography; it provides integrity by using digital signatures, and it authenticates via certificates.

The following considerations can help determine when SSL is the best option:

- Connections originate from a web browser.
- The IT department has limited or no control over the remote system or the client software, as in the case of a partner or customer.
- The enterprise needs to provide occasional, short-duration access from unmanaged or home computers, airport or library kiosks, or Internet cafés.
- Remote-access requirements include access to limited company network resources, not full network access.

Note: The preceding considerations for SSL VPN are referenced from http://cisco.com/en/US/partner/netsol/ns465/networking_solutions_white_paper0900aecd801b1b0f.shtml

SSL User Experience

Users who are accustomed to accessing applications via a web browser will not notice a difference when SSL is added to the network. Users must depend on Active X or Java Applets to access applications without a browser.

SSL Strengths

The strengths of SSL for secure remote access include the following:

- **Has low training overhead**—SSL enjoys broad support in commercial web browsers.
- **Supports existing and planned authentication methods**—Server plug-in software and SSL appliances support existing authentication methods, as well as mutual authentication using digital certificates.
- **Provides anywhere access**—SSL can be invoked via a web browser from any PC at any location: a trade-show kiosk, an Internet café, Wi-Fi hotspots, another company's network, and any other computer with Internet access. However, it is very important to note that due care must be taken to ensure that public endpoint use isn't compromised with malicious software, such as malware, spyware, key-loggers and so forth, rendering the public endpoint use insecure.
- **Reduces network interoperability issues**—Because the underlying protocol is the same one used for secure web transactions, an SSL VPN functions from any location with a web browser, including business-to-partners environments and through proxy servers, without changes to the underlying security infrastructure.
- **Has client ubiquity**—Client software is built in to the web browsers installed on almost all end-user devices, eliminating the need to install new VPN client software.
- **Offers transparent wireless roaming**—SSL sessions are not locked to an IP address.

When to Implement SSL

In the arena of providing secure connectivity to remote users, SSL is gaining momentum with the following advantages:

- The SSL-based VPN eliminates the need for separate client software. This reduces the installation, support, and system compatibility burden associated with installing and maintaining desktop software.
- The SSL-based VPN reduces network interoperability issues because the underlying protocol is the same as secure web transactions. An SSL/VPN will function anywhere there is a compatible web browser, including extranet environments and through proxy servers without changes to the underlying security infrastructure.
- For partner extranet access, SSL/VPNs are easier to deploy to allow partners access to a specific functionality on a network. The partner will not be required to install a VPN client, which may conflict with another VPN client already on the partner's PC, and

access can easily be restricted to specific resources on the network. Some client/server applications may be incompatible with the SSL/VPN.

Typically, IPsec interoperability among multiple vendors for remote access VPNs has not experienced a great deal of success. Combined with that is the set of difficulties encountered when IPsec client software has to interoperate with the standard desktop operating system and other application suites running on the client PC. SSL VPN allows you to overcome these difficulties.

Finally, for corporate remote access, some customers weigh whether an SSL VPN can solve all of their application needs, but most customers look at SSL VPN as an enhancement technology for remote access IPsec VPNs—and not as a replacement technology.

SSL VPN Considerations for Building Versus Buying

The main advantage of the SSL VPN is that it does not need remote client installation, and that makes SSL VPN deployment a less onerous task than IPsec VPN deployment. However, scaling at the head-end is quite a challenge because SSL is an end-to-end protocol, and having a server terminating thousands of simultaneous SSL connections does not provide a scalable solution. As a result, load sharing needs to be done at the head-end.

In addition, remote users should be trained on how to handle the remote end after the remote user finishes using an SSL VPN connection.

If you are building the SSL VPN, consider load sharing at the head-end as well as deep packet inspection of the incoming SSL traffic.

If you are buying the SSL VPN solution, it is best if the web-hosting company that is hosting your applications with HTTP access allows SSL access, too, as a part of the complete service bundle.

Drawbacks of SSL VPN

Certain deployment options of SSL demand certain precautions to help protect the remote user's security credentials. At a public Internet connection, for example, when an end user carries out banking activities over the Internet, all the residual user data must be cleaned up properly after the SSL session finishes. Otherwise, a malicious attempt to harvest user data after the user has finished the banking duties can become successful.

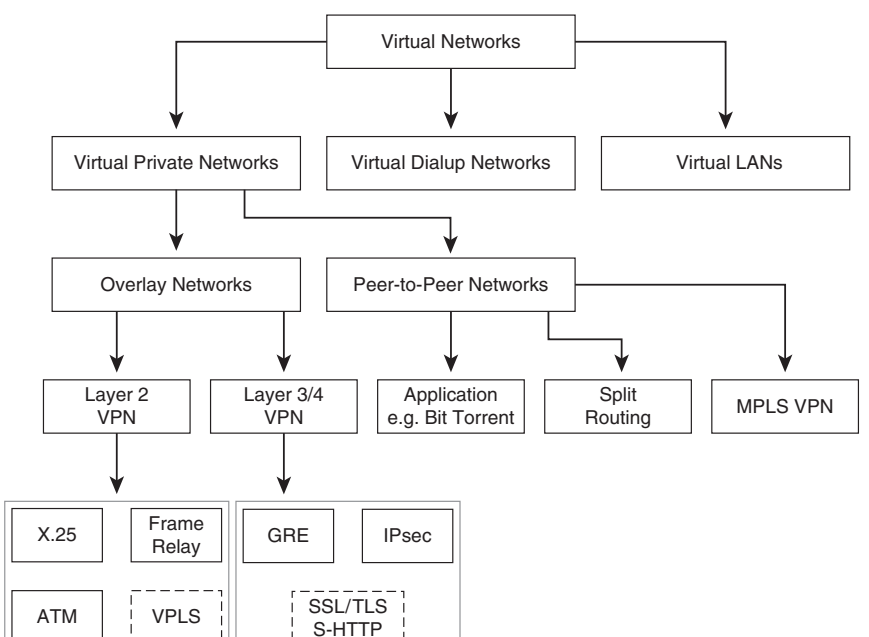
Not needing to install a VPN client is an advantage for SSL VPN, but at the same time only web-browser accessible applications can utilize SSL as a security protocol. There has been development in this area to allow users an "inside the main office" experience over SSL by making more than just web browsing applications secure.

Compromised endpoints on the Internet can receive SSL-encrypted signals from the Internet to initiate unethical activity such as a DDoS attack.

Classifying Virtual Private Networks

Figure 3-1 defines the place for MPLS, IPsec, and SSL VPN solutions under a hierarchy of virtual networks. Because it has become increasingly clear that building physical networks to cater to business needs is impractical, expensive, and slower-placed than the actual growth of business needs, virtual networks were conceived. This hierarchy helps to show the placement of each technology with respect to others.

FIGURE 3-1 Defining the Hierarchy for Virtual Private Networks



VPN is really an overlay network on a physical network infrastructure. For example, consider how the act of making a phone call to someone realizes the principle of creating a VPN between the calling parties. The physical network infrastructure from the telecommunication service provider goes to many homes and businesses, yet by dialing the other party's number, you create a virtual connection, or tunnel. This overlay network, known as VPN, is established only for the duration of the call, and at the same time, many other VPNs can be established on the same physical infrastructure without disrupting others.

A virtual private dial-up network (VPDN) allows the remote users to connect into the private network using a shared infrastructure. The VPDN is a cost-effective method of establishing a long-distance, point-to-point connection between remote dial users and a private network.

A virtual local-area network (VLAN) depicts a network of computers or endpoints connecting to the same virtual wire, even though physically the computers may be in different geographical locations. That VLANs are configured through software rather than hardware brings required flexibility.

An overlay network generally follows hub-and-spoke topologies for the connecting networks. Hubs represent connectivity to the centralized resources such as servers, whereas spokes represent the remote site connectivity having end stations or clients.

Peer-to-peer networks differ from the overlay network in that each workstation has equal capabilities and responsibilities.

Layer 2, Layer 3, and Layer 4 refer to the OSI stack.

Some examples of the Layer 2 networks are

- Layer 2 Forwarding (L2F)
- Layer 2 Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)

L2F was developed by Cisco Systems, Inc. and enables businesses to set up Layer 2 VPNs that use the Internet backbone to move packets. A very similar concept developed by Microsoft Corporation, U.S. Robotics, and others is PPTP. However, Microsoft and Cisco agreed to merge their respective protocols into a single, standard protocol called Layer 2 Tunneling Protocol (L2TP).

L2TP allows ISPs to operate VPNs at Layer 2 as well by using the best of both protocols, L2F and PPTP.

Some examples of Layer 3 and Layer 4 networks are

- IPsec
- Generic Routing Encapsulation (GRE)
- Secure Socket Layer (SSL)
- Split routing

The IPsec protocol is based on CIAN tenants, as discussed in Chapter 1, and provides encryption, integrity, authentication, and nonrepudiation capability to IP packets that lack standards required to secure the packets.

GRE is a tunneling protocol developed by Cisco Systems, Inc. that allows network layer packets to contain packets from a different protocol. It is widely used to tunnel protocols inside IP packets for VPNs, as well as encapsulate multicast traffic, because IPsec addresses only unicast IP packets. The most common use of GRE is to encapsulate, for example, non-IP, multicast traffic and then allow IPsec to encrypt it. So, in a sense, a GRE tunnel within an IPsec tunnel provides a tunnel within a tunnel. This is an inefficient way to transport protocols, but it facilitates overcoming issues of encapsulating traffic that IPsec does not natively support.

SSL is a protocol that encrypts Transmission Control Protocol (TCP) operating at Layer 4 of the OSI stack. Initially developed by Netscape, SSL allows a secure exchange between two workstations communicating over the Internet. Ratified under Transport Layer Security (TLS) by IETF, SSL version 3.0 represents the foundation on which TLS 1.0 was built. SSL and TLS utilize a cryptographic system that uses two keys to encrypt data—a public key known to everyone and a private or secret key known only to the recipient of the message. HTTP is often secured by SSL or TLS to carry out a secure transaction such as a credit card

information exchange. Secure HTTP (S-HTTP) is another protocol providing similar functionality to SSL. SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely; S-HTTP is designed to transmit individual messages securely. IETF has approved both protocols SSL and S-HTTP; they are complementary rather than competing technologies.

Finally, split routing is a routing technique to separate IP traffic so that VPNs can be created by separating traffic sourced from specific networks and destined to a designated destination.

Table 3-1 shows a direct comparison between MPLS, IPsec, and SSL in light of VPN solution deployment considerations and helps decision makers to select the appropriate technology to suit their business requirements.

TABLE 3-1 Comparison of MPLS, IPsec, and SSL Deployments

	MPLS-Based VPN	IPsec-Based VPN	SSL-Based VPN
Topology	Site-to-site VPN: Hub-and-spoke or full-mesh.	Site-to-site VPN: Mainly hub-and-spoke and dual hub for backup. Remote-access VPN: Mainly VPN head-end with redundancy.	Remote-access VPN: Endpoint to endpoint with load balancing at head-end.

TABLE 3-1 Comparison of MPLS, IPsec, and SSL Deployments

	MPLS-Based VPN	IPsec-Based VPN	SSL-Based VPN
IPsec Session Authentication	Establishes VPN membership during provisioning, based on logical port and unique route descriptor. Defines access to a VPN service group during service configuration, denies unauthorized access.	Authenticates through digital certificate or preshared key. Drops packets that do not conform to the security policy.	Handshake process with extension allows clients to initiate session with virtual server.
Confidentiality	Separates traffic, which achieves same results delivered in trusted Frame Relay or ATM network environments.	Uses a flexible suite of encryption and tunneling mechanisms at the IP network layer.	Encrypts traffic using standard symmetric ciphers.
Service-Level Agreements Based on Quality of Service	Enables SLA with a scalable, robust QoS mechanism and traffic engineering capability.	Does not address QoS and SLA directly, although Cisco IPsec VPN deployments can preserve packet classification for QoS within an IPsec tunnel.	Not applicable; service provider network is unaware of SSL traffic.

TABLE 3-1 Comparison of MPLS, IPsec, and SSL Deployments

	MPLS-Based VPN	IPsec-Based VPN	SSL-Based VPN
Scalability	Highly scalable because no site-to-site peering is required. Capable of supporting tens of thousands of VPNs over the same network.	Site-to-site VPN: Acceptable scalability in most typical hub-and-spoke deployments. Scalability becomes challenging for a very large, fully meshed IPsec VPN deployment; may require supplemental planning and coordination to address key distribution, key management, and peering configuration. Remote-access VPN: Scalability at the head-end is addressed with VPN concentrator type of device.	Load-balancing required at the head-end because SSL requires end point-to-end point connection. Not applicable on the client site because service provider network is unaware of SSL traffic.

TABLE 3-1 Comparison of MPLS, IPsec, and SSL Deployments

	MPLS-Based VPN	IPsec-Based VPN	SSL-Based VPN
Management	MPLS monitoring, traffic engineering required. Requires one-time provisioning of customer edge and provider edge devices to enable the site to become a member of an MPLS VPN group.	Reduces operational expense through centralized network-level provisioning for IPsec VPN terminating on CPE. Uses centralized provisioning for IPsec VPN terminating in the network equipment. Typically mapping to designated instance of MPLS VRF. Can be deployed across any existing IP networks or the Internet. Head-end needs to ensure that IPsec connection initiated IKE sessions per second and number of simultaneous IKE negotiations can be processed.	No need to manage client, because SSL support is standard from endpoints. Head-end needs monitoring and capacity management to ensure that SSL connection per second and number of simultaneous SSL connections can be terminated at the head-end.

TABLE 3-1 Comparison of MPLS, IPsec, and SSL Deployments

	MPLS-Based VPN	IPsec-Based VPN	SSL-Based VPN
VPN Client	Transparent to the endpoint because label-switching knowledge is not required. MPLS VPN is a network-based VPN service; users do not need VPN clients to interact with the network.	Is required for client-initiated IPsec VPN deployments. Cisco VPN client software is supported by Microsoft Windows, Solaris, Linux, and Macintosh operating systems.	Is not required; relies on web browser.
Place in Network	Core network.	Local loop, edge, and off net.	Local loop, edge, and off net.
Transparency	Resides at the network layer. Transparent to applications.	Resides at the network layer. Transparent to applications.	Resides at the session layer. Currently, many TCP-based applications work with SSL; however, voice and video services for remote clients generally do not run over SSL connection.

Summary

MPLS VPN provides security as defined by the legacy technology, such as Frame Relay and ATM. MPLS integrates Layer 2 information about network links such as bandwidth, latency, and utilization into Layer 3 (IP) within a service provider's network to simplify and improve IP-packet exchange.

Building an MPLS VPN provides an efficient transport mechanism of interconnecting business networks, yet provides separation of traffic from other business traffic traversing on the shared infrastructure. MPLS VPNs are flexible because the high availability required for businesses to operate is provided by diverting and routing traffic around link failures, congestion, and bottlenecks.

In addition to data separation, MPLS VPNs also provide quality of service to manage different kinds of data streams based on traffic priority and the business service plan.

IPsec VPN provides the most robust remote access environment to remote users by extending almost any data, voice, or video application available in the office to remote working locations. IPsec VPN client software on the remote system enables a user experience and workflow consistent with the office environment by providing easy application access and system integrity enforcement. IPsec VPN provides the most comprehensive level of network access to remote users, thus extending the productivity of the office to virtually any location. This "any

application access" has made IPsec VPN the de facto standard for extending connectivity to home offices, traveling employees, remote workers, and day extenders.

SSL-based VPN is a comparatively new technology that provides remote access connectivity from almost any Internet-enabled location using a web browser and its native SSL encryption. Although application accessibility is constrained relative to IPsec VPNs, SSL-based VPNs allow for access to a growing set of common software applications. SSL-based VPN requires slight changes to user workflow because some applications are presented through a web-browser interface, not through their native GUI. Client/server application support generally requires specific and sometimes browser-dependent applets to be dynamically downloaded to the remote system. Using web technology for connectivity allows accessibility from almost any Internet-connected system without needing to install additional desktop software. Because SSL-based VPN can provide network access to users from almost any Internet-connected system, it is an emerging option for extending remote access to users who require access to specific applications.