ENTERPRISE GUIDE FOR SELECTING AN IP VPN ARCHITECTURE—COMPARING MPLS, IPSec, AND SSL

The Layer 3 IP VPN architecture that an enterprise chooses for its corporate WAN has wide-ranging effects on the business, including scalability, connectivity options, and the ability to deploy voice, video, and multicast applications. Enterprises can select from Layer 3 IP VPN architectures based on Multiprotocol Label Switching (MPLS), IP Security (IPSec), and Secure Sockets Layer (SSL).

THE OPTIMAL IP VPN ARCHITECTURE FOR AN ENTERPRISE CORPORATE WAN DEPENDS ON ITS BUSINESS REQUIREMENTS

INTRODUCTION
Companies selecting an IP VPN architecture—MPLS, IPSec, and SSL—need to consider their business needs because there is no single best choice. In fact, many enterprises are best served by some combination of the three architectures. The choice of architecture has wide-reaching effects, including flexibility and whether the VPN will be network-based or customer premises equipment (CPE) based. MPLS-based VPNs are usually offered by the service provider as a managed service, and originate and terminate in the service provider’s MPLS-enabled IP network. IPSec and SSL VPNs, in contrast, are typically managed by the enterprise, and originate and terminate at the CPE. IPSec- and SSL-based VPNs are also available as a managed service from certain service providers.

This white paper describes each Layer 3 IP VPN architecture—MPLS, IPSec, and SSL—and explains each technology’s strengths and limitations, and suggests when it might be the best choice for an enterprise. The paper concludes with a table that compares and contrasts the architectures.

CRITERIA FOR EVALUATING IP VPN ARCHITECTURES FOR THE ENTERPRISE
The primary function of an IP VPN is to provide cost-effective, secure connectivity over a shared infrastructure with the same or better policies and service attributes that the enterprise enjoys within its dedicated private network. To achieve this goal, the IP VPN solution must deliver the following essential attributes: high availability, network security, quality of service (QoS), scalability, and ease of management. Different IP VPN architectures deliver these attributes to varying degrees, so the best choice for a given enterprise depends on the relative importance of the following business needs.

High Availability: Deliver Data in a Reliable and Timely Manner
An IP VPN needs to predictably deliver high service availability for enterprise users and their partners and customers—a capability that requires high network reliability as well as redundancy. Some service providers are able to offer service-level agreements (SLAs), usually for an additional fee. Service provider SLAs define the specific terms or metrics regarding availability of networking resources, and offer the VPN subscriber a contractual guarantee for network uptime and performance. An SLA can optionally define multiple levels of service for different types of traffic, such as voice and data, with lower-cost alternatives for less critical traffic.
Security: Keep Company Data Confidential as It Travels Over a Shared Infrastructure

As multiple companies share the same service provider’s shared core network, they need to know that their own VPN will remain private—that is, that the traffic from one company’s VPN will never flow onto another company’s VPN. This requirement not only protects privacy and security, it helps companies comply with industry regulations such as the Sarbanes-Oxley Act and the Health Insurance Portability and Protection Act (HIPPA) in the United States, the Data Protection Act in the United Kingdom, and others. To ensure that every VPN on the shared core network remains private, service providers use a variety of security mechanisms, including: tunneling, encapsulation, encryption, constrained routing distribution, routing-table separation between VPNs, traffic separation, packet authentication, user authentication, and access control.

QoS: Prioritize by Traffic Type

Network QoS pertains to latency, jitter, and packet loss—metrics that determine the quality of the services delivered over the network from end to end. A related network attribute, class of service (CoS) defines the specific level of service required for different traffic types, such as voice, video, or data. Enterprises that deliver mission-critical applications over the VPN typically look for a service provider that offers multiple CoS. The QoS mechanisms within the VPN enable multiple CoS by classifying traffic types and assigning priority to those that are mission-critical or delay-sensitive, such as voice and video. QoS mechanisms also enable the VPN to manage congestion across varying bandwidth rates.

Enterprises that out-task VPN service management typically can choose from three CoS: gold class for controlled latency, silver class for controlled load, and bronze class for best effort. Some service providers have recently begun offering more granular CoS, including:

- Level 4: Real time (voice, interactive video)
- Level 3: Business interactive (call signaling, Systems Network Architecture [SNA], Oracle, PeopleSoft, SAP, Telnet, and others)
- Level 2: Real time (streaming video, network management)
- Level 1: Business LAN-to-LAN (Internet Web, IBM Lotus Workplace, Novell Groupwise, and others)
- Level 0: Best-effort data (Simple Mail Transfer Protocol [SMTP], FTP, Internet Web, and others)

For each CoS, the provider meets specified criteria for latency, jitter, and packet loss.

Scalability: Adapt to Meet Changing Bandwidth and Connectivity Needs

Enterprise bandwidth and connectivity needs change over time, sometimes suddenly, as the business expands, consolidates, merges, or begins encouraging telecommuting. A need for extranet connectivity to partners or customers also boosts bandwidth and connectivity requirements. To remain agile, the enterprise needs to choose a service provider with the ability to scale the VPN to accommodate unplanned growth and changes.

Management: Extend Access to Different Sites and Contain Administrative Costs

Management of the VPN spans headquarters, remote branches, and sometimes mobile workers and teleworkers. The VPN architecture an enterprise chooses can affect manageability and associated cost. The types of management services enterprises need can include:

- Provisioning
- Distributing and installing VPN-enabled CPE and VPN client software, if needed
- Installing security and QoS policies
- Supporting SLAs
- Preserving route type and route metric elements
- Supporting current and future unicast IP routes
- Supporting noncontiguous networks across VPN sites
- Facilitating network-performance management, fault identification and resolution, billing, reporting, as well as service addition, removal, and change functions

**MPLS-BASED VPNS**

**Description**

MPLS blends the intelligence of routing with the performance of switching, providing significant benefits to service providers with existing native IP architectures, existing native IP plus ATM architectures, or a mixture of other Layer 2 technologies. MPLS-based Layer 3 VPNs conform to a peer-to-peer model that uses Border Gateway Protocol (BGP) to distribute VPN-related information. They are based on the Internet Engineering Task Force (IETF) RFC 2547bis specification for BGP, which defines a VPN solution that uses MPLS to forward customer traffic using per-customer labels. BGP distributes route information across the provider’s backbone network so that the provider participates in and manages customer routing information.

A primary advantage of MPLS is that it provides the scalability to support both small and very large-scale VPN deployments: up to tens of thousands of VPNs on the same network core (see Figure 1). In addition to scalability, its benefits include end-to-end QoS, rapid fault correction of link and node failure, bandwidth protection, and a foundation for deploying additional value-added services. MPLS technology also simplifies configuration, management, and provisioning, helping service providers to deliver highly scalable, differentiated, end-to-end IP-based services. For example, the service provider can offer SLAs by enabling MPLS traffic engineering and fast reroute capabilities in the core network. In conjunction with the MPLS VPN service offering, service providers can also offer a multicast service, which is the replication of packets from a single source to multiple destinations, enabling voice or video broadcasts, for instance.

**Figure 1**

Site-to-Site MPLS-Based VPN
Indicators That MPLS Is a Good Choice

- The company needs SLAs.
- 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, and therefore must ensure that delay-sensitive traffic, such as voice, video, or mission-critical data, receives 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.

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.

MPLS Strengths

- Network security—MPLS enforces traffic separation between different VPNs on the same core network by using route distinguishers. Unique route distinguishers are assigned automatically when the VPN is provisioned and are 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.\(^1\) 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 only needs to establish local peering 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.

---

IPSEC-BASED VPNS

Description
IPSec protocol, a suite of IETF open standards, provides the framework for CPE-based Layer 3 VPNs. To protect data as it travels across a public or a closed IP network, IPSec supports a combination of the following network security functions:

- Data confidentiality—Encrypts packets before transmission
- Data integrity—Authenticates packets to help ensure that the data has not been altered during transmission
- Data origin authentication—Authenticates the source of received packets, in conjunction with data integrity service
- Antireplay—Detects aged or duplicate packets, rejecting them to avoid replay attacks

The IPSec standard also defines several new packet formats, such as encapsulating security payload (ESP), for confidentiality. ESP supports any type of symmetric encryption, including standard 56-bit Data Encryption Standard (DES), the more secure Triple DES (3DES), and the emerging Advanced Encryption Standard (AES). IPSec parameters are communicated and negotiated between network devices in accordance with the Internet Key Exchange (IKE) protocol.

The IPSec protocol provides protection for IP packets by allowing network designers to specify the traffic that needs protection, define how that traffic is to be protected, and control who can receive the traffic. IPSec VPNs replace or augment existing private networks based on traditional WAN infrastructures such as leased-line, Frame Relay, or ATM. They fulfill the same requirements as these WAN alternatives including the support for multiple protocols. The advantage of IPSec is that it meets network requirements more cost effectively and with greater flexibility by using today's most pervasive transport technologies: the public Internet and service providers' IP-based networks.

When an enterprise out-tasks IPSec VPN service management, the service provider typically configures IPSec in a hub-and-spoke topology, where all branches (spokes) maintain a point-to-point connection to the hub, or headend (see Figure 2). IPSec inherently supports IP unicast. Enterprises that need other Layer 3 protocols, such as AppleTalk or IPX, can use protected generic routing encapsulation (GRE) tunnels over IPSec.

IPSec is suitable for both site-to-site (Figure 2) and remote-access (Figure 3) VPNs.

Figure 2
Site-to-Site IPSec-Based VPN
Indicators That IPSec Is a Good Choice
The following factors help enterprises to determine when to use IPSec.

- The enterprise needs security measures like 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 their 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.

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

Remote Access
Typically, the user invokes the VPN software client and selects the appropriate destination, such as a host name or IP address. Upon 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 any modifications to the hosted site or client.
Site to Site
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:

- **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**—Headend 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.

SSL-BASED VPNS

Description
Secure Sockets Layer (SSL) is an emerging alternative to IPSec for remote-access VPNs (see Figure 4). It is not designed for site-to-site VPNs. SSL provides access to Web-based applications from any location with a Web browser, an Internet connection, and without special client software. It provides secure connectivity by authenticating the communicating parties and encrypting the traffic that flows between them. Because SSL operates at the session layer, it works only with those applications coded for SSL, such as Web browsers and Web-based e-mail. SSL-based VPNs do not support applications not coded for SSL, including standard e-mail clients, Telnet, FTP, IP telephony, multicast applications, and applications requiring QoS.
An advantage of SSL as a remote-access VPN solution is that it does not require any special VPN client software other than a Web browser. In addition, the enterprise IT group or service provider can provide granular access control, limiting individual users’ access to specific Web pages or other internal resources.

IT infrastructure requirements for SSL-based VPNs include application proxies because SSL must be aware of each individual connection or application session. In addition, the headend needs adequate memory to maintain all individual application connections. SSL is computing-intensive because of encryption processes, so the server needs adequate processing and memory resources to avoid becoming a bottleneck.

Most enterprises regard SSL VPN as an enhancement to IPSec VPN for remote access, not as a replacement. Its simplified remote client implementation and management make it a good choice for partner VPN connectivity when the enterprise does not control the remote client. When enterprises deploy both SSL and IPSec for their VPNs, they generally use SSL to provide limited-duration access to Web-based applications from unmanaged or home computers, airport or library kiosks, and Internet cafés; and they use IPSec for remote access from corporate-managed computers to provide full network access, providing users with the same experience they would have in the office.
Indicators That SSL is a Good Choice
The following considerations can help determine when SSL is the best option:

- Connections originate from a Web browser.
- 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.

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

SSL Strengths
The strengths of SSL for secure remote access include:

- Low training overhead—SSL enjoys broad support in commercial Web browsers.
- Support for 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 tradeshow kiosk, Internet café, WiFi hotspots, another company’s network, and any other computer with Internet access.
- 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 any changes to the underlying security infrastructure.
- 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.
- Transparent wireless roaming—SSL sessions are not locked to IP.

IP VPN ARCHITECTURE COMPARISON
Table 1 shows the advantages and limitations of managed services based on the three architecture options: MPLS, IPSec, and SSL.
### Table 1. MPLS, IPSec, and SSL Comparison

<table>
<thead>
<tr>
<th></th>
<th>MPLS-Based VPN</th>
<th>IPSec-Based VPN</th>
<th>SSL-Based VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Topology</strong></td>
<td>Site-to-site VPN: Hub-and-spoke or full-mesh</td>
<td>Site-to-site VPN: Mainly hub-and-spoke</td>
<td>Remote-access VPN</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Session authentication</strong></td>
<td>Establishes VPN membership during provisioning, based on logical port and unique route descriptor</td>
<td>Authenticates through digital certificate or preshared key</td>
<td>Authenticates through digital certificate</td>
</tr>
<tr>
<td></td>
<td>Defines access to a VPN service group during service configuration; denies unauthorized access</td>
<td>Drops packets that do not conform to the security policy</td>
<td></td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
<td>Separates traffic, which achieves same results delivered in trusted Frame Relay or ATM network environments</td>
<td>Uses a flexible suite of encryption and tunneling mechanisms at the IP network layer</td>
<td>Encrypts traffic using the public key infrastructure (PKI)</td>
</tr>
<tr>
<td><strong>QoS and SLAs</strong></td>
<td>Enables SLAs with a scalable, robust QoS mechanism and traffic-engineering capability</td>
<td>Does not address QoS and SLAs directly, although Cisco® IPSec VPN deployments can preserve packet classification for QoS within an IPSec tunnel</td>
<td>Not applicable; service provider network is unaware of SSL traffic</td>
</tr>
<tr>
<td><strong>Scalability</strong></td>
<td>Highly scalable because no site-to-site peering is required</td>
<td>Acceptable scalability in most typical hub-and-spoke deployments</td>
<td>Not applicable; service provider network is unaware of SSL traffic</td>
</tr>
<tr>
<td></td>
<td>Capable of supporting tens of thousands of VPNs over the same network</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Site-to-site support</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Remote access support</strong></td>
<td>Yes, if used in conjunction with IPSec</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Provisioning</strong></td>
<td>Requires one-time provisioning of customer edge and provider edge devices to enable the site to become a member of a MPLS VPN group</td>
<td>Reduces operational expense through centralized network-level provisioning for CPE-based service offering</td>
<td>Not applicable; service provider network is unaware of SSL traffic</td>
</tr>
<tr>
<td></td>
<td>Needs MPLS-enabled network elements at the core and edge of the service provider network</td>
<td>Uses centralized provisioning for network-based service offering</td>
<td></td>
</tr>
<tr>
<td><strong>Service deployment</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>VPN client</strong></td>
<td>Is not required because MPLS VPN is a network-based VPN service; users do not need VPN clients to interact with the network</td>
<td>Is required for client-initiated IPSec VPN deployments</td>
<td>Is not required; relies on Web browser</td>
</tr>
<tr>
<td></td>
<td>Cisco VPN client software is supported by Microsoft Windows, Solaris, Linux, and Macintosh operating systems</td>
<td>Cisco VPN client software is supported by Microsoft Windows, Solaris, Linux, and Macintosh operating systems</td>
<td></td>
</tr>
<tr>
<td><strong>Place in network</strong></td>
<td>Core network</td>
<td>Local loop, edge, and off-net</td>
<td>Local loop, edge, and off-net</td>
</tr>
<tr>
<td><strong>Transparency</strong></td>
<td>Resides at the network layer transparent to applications</td>
<td>Resides at the network layer transparent to applications</td>
<td>Resides at the session layer works only with applications coded for SSL</td>
</tr>
</tbody>
</table>

**CONCLUSION**

Enterprises can meet their site-to-site VPN business requirements with MPLS, IPSec, or a combination, and their remote-access VPN requirements with a combination of IPSec and SSL. To find providers of managed VPN services...
based on MPLS, IPSec, and SSL, look for the Cisco Powered logo. Service providers that display this logo are recommended by Cisco Systems®. They use Cisco equipment in their networks end to end, and meet Cisco standards for network performance, service, and support. They supply reliable, industry-leading services that help enable advanced applications. About 380 of the most successful service providers worldwide are members of the Cisco Powered Network Program. Situated in more than 56 countries, these program members offer a wide range of services for small and large businesses alike.

For more information about the Cisco Powered Network Program, visit http://www.cisco.com/cpn. This site includes a convenient search tool for identifying a local service provider with the Cisco Powered Network designation, as well as descriptions of all of the types of services that can carry the Cisco Powered Network designation.

For more information about managed VPN services, visit http://www.cisco.com/go/managedservices.

To view an e-tour of managed services, visit http://www.cisco.com/go/msetour.