White Paper

Comparing MPLS-Based VPNs, IPSec-Based VPNs, and a Combined Approach from Cisco Systems

In today's shifting economy, service providers' revenue and profitability hinge on delivering managed network services in addition to connectivity services. The global market for managed VPN services, for example, is expected to top US$21 billion by 2007, according to Ovum, a market research and consulting firm. Managed VPN services provide the foundation for additional value-added services such as managed IP telephony, managed security, hosted applications, e-commerce, content delivery, disaster recovery, integrated access, and multimedia applications. The type and deployment of the service provider's prevailing Layer 3 IP VPN (L3VPN) architecture—Multiprotocol Label Switching (MPLS)-based VPN, IP Security (IPSec)-based VPN, or a combination—influence the service provider's market coverage, service offerings, incremental value-added services, and revenue potential.

This white paper compares MPLS- and IPSec-based L3VPN architectures. It begins by exploring the L3VPN mechanisms developed by the IETF and summarizing the general objectives of VPNs. Next it presents the relative strengths of MPLS- and IPSec-based VPNs and explains how service providers can use both architectures for optimum advantage. The white paper concludes with a brief description of the range of VPN infrastructure solutions available from Cisco Systems®: the Cisco® Network-Based MPLS VPN solution, the Cisco IPSec CPE VPN solution, and the Cisco Network-Based IPSec VPN solution, which combines MPLS-based and IPSec-based technologies.

Survey of IETF L3VPN Mechanisms

In recent years, several IETF working groups have focused on VPN techniques pertaining to Internet security, label switching standardization for efficient packet forwarding, and provider-provisioned Layer 3-routed VPN mechanisms. Key efforts include the following:

- The IETF MPLS working group, under the routing area, is developing mechanisms for using label switching and implementing label-switched paths over various packet-based, link-level technologies. This working group is also exploring procedures and protocols for distributing labels between routers, and for using encapsulation to preserve and isolate multiple VPNs in the peer model environment.

- The IETF IPSec working group, under the security area, is designing cryptographic security mechanisms that can flexibly support combinations of authentication, integrity, access control, and confidentiality in the overlay model environment.
- The IETF L3VPN working group, under the Internet area, is defining and specifying standards for a finite set of solutions for supporting provider-provisioned L3VPNs. These solutions include Border Gateway Protocol (BGP)/MPLS IP VPNs, IP VPNs using virtual routers, and customer edge-based VPNs using IPSec.

These L3VPN mechanisms are complementary rather than competitive. In fact, many service providers can increase their service footprint and gain other competitive advantages by combining VPN architectures and taking advantage of their respective strengths. The Cisco Network-Based IPSec VPN solution, described later in this paper, combines both architectures to enable service providers to expand their VPN portfolio with secure on-net and off-net remote access and remote site-to-site services.

Essential Attributes of VPNs

The service goal of VPNs is to provide cost-effective, secure connectivity over a shared infrastructure with the same policies and service attributes enjoyed within a dedicated private network. To achieve this goal, a VPN solution must deliver the following essential attributes: quality of service (QoS), ease of management, security, high availability, and scalability.

QoS: Prioritize by Traffic Type

Where QoS refers to the overall quality of the services being delivered over the network, class of service (CoS) defines the specific level of service required for a traffic type: voice, video, or data. As more enterprises demand secure, converged infrastructures, service providers need to offer multiple classes of service to support mission-critical applications. The QoS mechanisms within the VPN fulfill this need by differentiating among traffic types and assigning priority to mission-critical or delay-sensitive traffic, such as voice and video. QoS mechanisms also enable the VPN to manage congestion across varying bandwidth rates.

Service providers today typically offer three classes of service: gold class for controlled latency, silver class for controlled load, and bronze class for best effort. Recently, enterprises have begun requesting more granular classes of service, 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, providers must be able to meet the latency, jitter, and packet-loss criteria specified in the service-level agreement (SLA), and implement pricing and QoS reporting schemes that correspond with the offered CoS.

Management: Quickly Fulfill Orders and Support SLAs

To offer network-based IP VPN services, service providers need carrier-class, centralized, scalable management capabilities for locations that might include the customer headquarters office, remote branches, teleworkers, and often the customer's business partners' offices. Primary management capabilities include:

- Provisioning
- Distributing and installing VPN-enabled customer premises equipment (CPE) and VPN software clients where 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 performance management, fault identification and resolution, billing, reporting, as well as service addition, removal, and change functions

The service provider's operations support system (OSS) provides these capabilities. An OSS with automated flow-through provisioning systems, and reporting and monitoring capabilities enables service providers to quickly fulfill VPN orders and support SLAs.

Security: Protect Against Intrusion and Tampering, and Isolate Each Customer's Data

It is essential that the VPN protect sensitive customer data so that it remains confidential across a shared infrastructure. This means that while all VPNs and the network core can share a single overlapping address space, the traffic from one VPN must never flow onto another VPN, and each VPN's routing information must remain separate and discrete.

VPNs also must be resistant to denial-of-service (DoS) attacks and intrusion. Effective security mechanisms used to protect VPNs include: tunneling, encapsulation, encryption, constrained routing distribution, routing table separation between VPNs, traffic separation, packet authentication, user authentication, and access control.

High Availability: Deliver Data in a Reliable and Timely Manner

A VPN needs to predictably deliver the high service availability that business customers expect and depend on—a capability that requires high network reliability, as well as redundancy. When high-availability mechanisms are built into a service provider's network, the provider can deliver SLAs as a premium service. SLAs define the specific terms or metrics regarding availability of resources, and offer the VPN subscriber a contractual guarantee for network uptime. A single SLA can optionally define multiple levels of service for different types of traffic, with lower-cost alternatives for less-critical traffic.

Scalability: Adapt to Meet Changing Bandwidth and Connectivity Needs

A service provider's VPN deployments might range from small office configurations to large enterprise implementations spread across regional or national boundaries. Therefore, the VPN architecture must adapt to meet customers' ever-changing bandwidth and connectivity needs. Additionally, in today's fiercely competitive, dynamic market environment, service providers must be able to deploy and provision large service requests rapidly. This requires the ability to scale the VPN to accommodate for unplanned growth and changes driven by customer demand. Service providers that can support a very large number of VPNs over the same network benefit from economies of scale and maximize their profit potential.

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, as well as those with existing native IP and ATM or a mixture of other Layer 2 technologies. MPLS extends the capabilities of IP to enable very large-scale implementations of VPNs. In addition to scalability, its benefits include end-to-end QoS, the ability to take advantage of existing networks to meet future growth, and rapid fault correction of link and node failure. MPLS technology also simplifies configuration, management, and provisioning, helping service providers deliver highly scalable, differentiated, end-to-end IP-based services.

MPLS-based L3VPNs use a peer-to-peer model that uses BGP to distribute VPN-related information. They are based on the 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, so that the provider participates in and manages customer routing information.

To offer premium VPN services bundled with SLA, service providers can enable MPLS traffic engineering and fast reroute (FRR) capabilities in the core network. To offer broadcast video or voice to multiple locations, service providers can deploy a multicast-enabled VPN. QoS-based VPNs offer three or more classes of service.

MPLS Strengths

The following are the primary strengths of MPLS-based VPNs:

- *Scalability*—A well-executed MPLS-based VPN deployment is capable of supporting tens of thousands of VPNs over the same network. MPLS-based VPNs scale well because they do not require the full-mesh, end-to-end site peering across the network.
- *Security*—MPLS provides traffic separation between VPNs by using unique route distinguishers. Route distinguishers are assigned automatically when the VPN is provisioned and are placed in packet headers to provide traffic separation. They are not seen by end users within the VPN group. MPLS VPN privacy is similar to the privacy in traditional WAN infrastructures such as Frame Relay and ATM. Miercom, which provides independent testing and analysis of networking services, has demonstrated that MPLS allows VPNs to be created through the core while providing security through data isolation. Additionally, networks can be designed so that customer routers have no knowledge of the core network, and likewise, the core routers have no knowledge of the customer edge. For a copy of the Miercom report, see:

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns103/c654/cdccont_0900aecd800c552e.pdf

- *Traffic engineering*—By deploying traffic engineering in the core, service provider network engineers can implement policies to help ensure optimal traffic distribution and improve overall network utilization. MPLS enables traffic engineering by allowing traffic to be directed through a specific path based on least-cost routing, link utilization, latency, jitter, and other factors.
- *Support for SLAs*—A well-executed MPLS-based VPN implementation supports SLAs and service-level guarantees (SLGs) by providing scalable, robust QoS mechanisms, guaranteed bandwidth, and traffic engineering capabilities.

IPSec-Based VPNs

Description

IPSec protocol, a framework of open standards, provides any combination of the following network security services:

- *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) standard, 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. IPSec VPNs fulfill the same requirements as these WAN alternatives, such as support for multiple protocols, high reliability, and scalability. 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, service provider IP backbones, and MPLS-based networks.

IPSec Strengths

The primary strengths of IPSec-based VPN are:

- *Security*—IPSec helps ensure data privacy with a flexible suite of encryption and tunneling mechanisms that protect packets as they travel over the network. Users are authenticated with digital certificates or preshared keys. Packets that do not conform to the security policy are dropped.
- *Ease of deployment*—IPSec enables fast time to market because it can be deployed across any existing IP network with little or no change to the existing IP network infrastructure.
- *Geographic reach*—An IPSec VPN can greatly increase the service provider's reach because it can take advantage of the Internet. Therefore, the service provider does not need to invest in infrastructure outside of its existing footprint.

MPLS-Based VPN Location

MPLS-based VPNs are deployed primarily within a service provider's network (see Figure 1), and can also be used to create an intranet or extranet. When used to create an intranet, MPLS-based VPNs link a corporate headquarters to multiple remote offices securely over a shared network, offering a cost-effective alternative to traditional leased-line, ATM, and Frame Relay technologies. For extranets, MPLS-based VPNs provide the flexible, policy-based connectivity needed to link the subscriber's business partners and customers. Table 1 compares MPLS-based VPNs with IPSec-based VPNs.

IPSec-Based VPN Location

IPSec-based VPNs are most useful at the local loop, edge, and outside of a service provider's network (off-net), where there is a higher degree of exposure to breach of data privacy and where IPSec mechanisms, such as tunneling and encryption, can best be applied. IPSec VPNs also can be deployed on the service provider's native IP network, securely connecting customer locations in an overlay model. From a services perspective, IPSec is especially useful for securing remote access and remote site VPN connections to the corporate network.

Figure 1
Network Location for IPSec and MPLS-Based VPNs

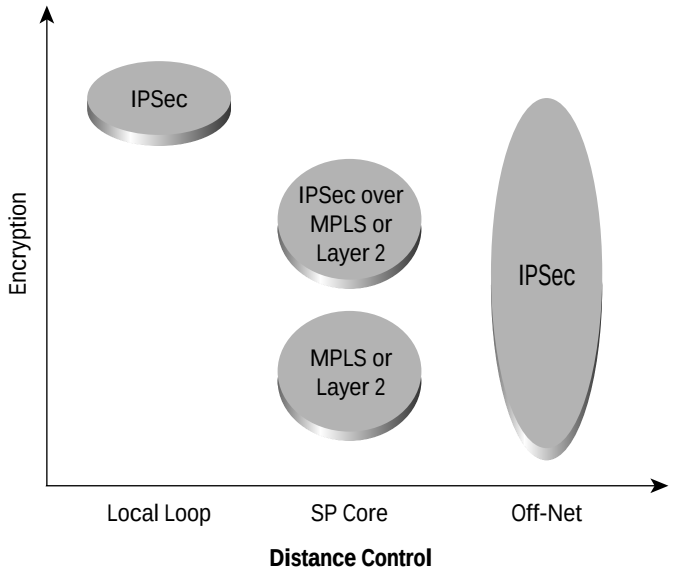


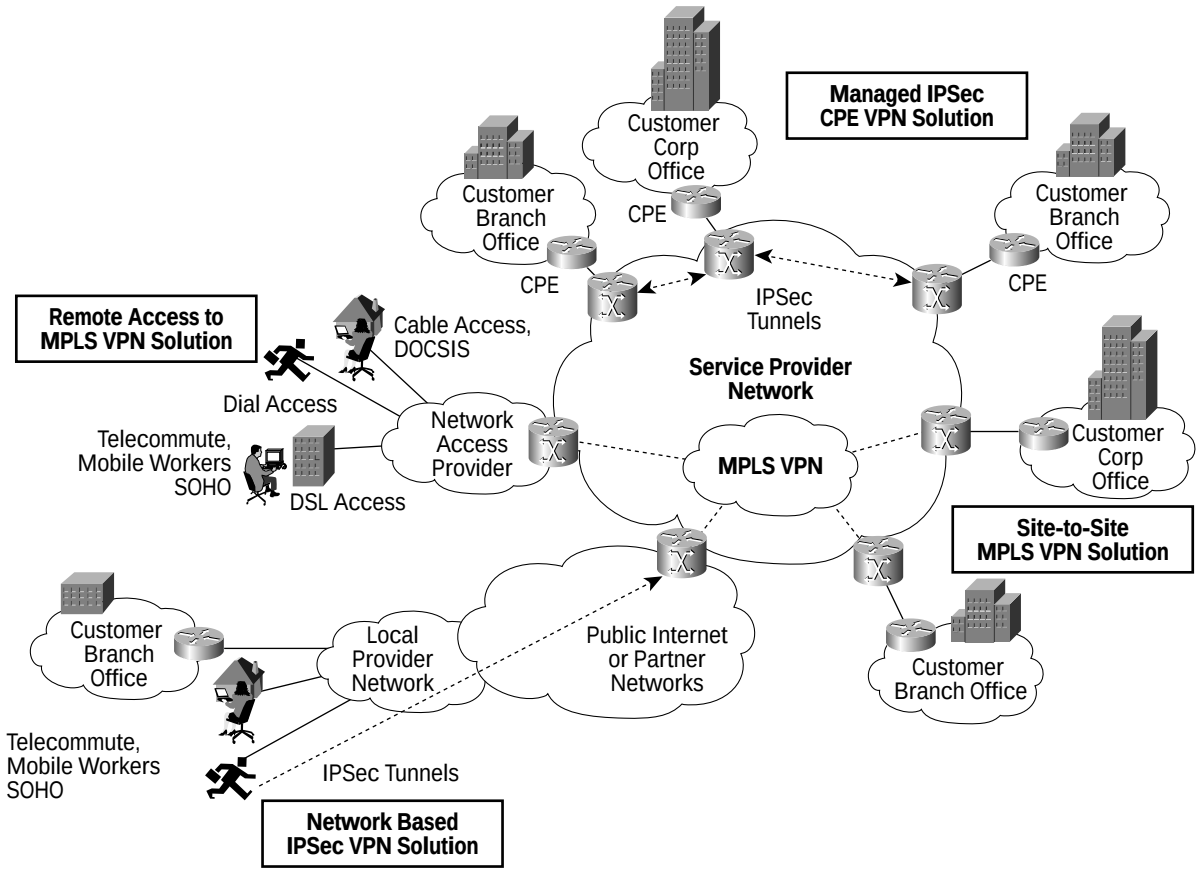
Table 1 Comparing MPLS- and IPSec-Based VPNs

	MPLS-Based VPN	IPSec-Based VPN
Place in Network	Core Network	Local Loop, Edge, and Off-Net
Transparency	Resides in the IP, ATM, or IP environment Transparent to applications	Resides at the network layer Transparent to applications
Scalability	Highly scalable because no site-to-site peering is required Capable of supporting tens of thousands of VPNs over the same network	For very large deployments, requires supplemental planning and coordination to address key distribution, key management, and peering configuration Scalability becomes challenging for a very large, fully meshed IPSec VPN deployment
Provisioning	Requires one-time provisioning of customer edge and provider edge devices to enable the site to become a member of a MPLS VPN group	Reduces operational expense through centralized network-level provisioning for CPE-based service offering Uses centralized provisioning for network-based service offering
Service deployment	Needs MPLS-capable network elements at the core and edge of the service provider network	Enables fastest time to market Can be deployed across any existing IP networks
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 via digital certificate or preshared key Drops packets that do not conform to the security policy
Confidentiality	Separates traffic, for 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
QoS and SLAs	Enables SLAs with a scalable, robust QoS mechanism and traffic engineering capability	Does not address QoS and SLAs directly, although Cisco IPSec VPN deployments can preserve packet classification for QoS within an IPSec tunnel
VPN client	Is not required because MPLS VPN is a network-based VPN service; users do not need VPN clients in order 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

Cisco VPN Technologies and Solutions

Cisco Systems offers end-to-end solutions for deploying a broad set of VPN architectures (see Figure 2). Solution components include VPN-enabled routers, WAN switches, VPN concentrators, access servers, and firewalls, as well as the Cisco IOS® Software and the Cisco IP Solution Center—a carrier-class VPN management and provisioning software suite. Following are descriptions of Cisco VPN architecture solutions that use MPLS and IPSec singly and in combination.

Figure 2
Cisco VPN Architecture Solutions



Cisco Site-to-Site MPLS VPN Solution

The Cisco Site-to-Site MPLS VPN solution enables service providers to offer secure data, voice, and video communications between corporate locations, with QoS guarantees. To meet the varying needs of small, medium, and large customers, service providers can offer this affordable solution with several access technologies, and speeds from 64K to STM-1. Service providers also have the option to offer site-to-site MPLS VPNs as a bundled offering with managed CPE, or as an unbundled offering without managed CPE.

The Cisco Site-to-Site MPLS VPN solution can be provisioned over either an MPLS core or the service provider's existing IP core. In the latter case, the subscriber's VPN is identified using either Layer 2 Tunneling Protocol version 3 (L2TPv3) or generic routing encapsulation (GRE). The flexibility to deploy the Cisco Site-to-Site MPLS VPN solution over either an MPLS core or IP core decouples the core technology from additional services, making it easier for the service provider to migrate from native IP to MPLS in the core.

Cisco Remote Access to MPLS VPN Solution

The Cisco Remote Access to MPLS VPN solution enables service providers to offer managed VPN services to the subscriber's remote users. By extending existing MPLS VPN capabilities, such as remote access to the last mile—over dial-up, digital subscriber line (DSL), or cable—service providers can achieve a higher return on investment (ROI) for existing MPLS core infrastructures. After the remote-access MPLS VPNs has been deployed, the service provider can extend its service portfolio by offering incremental value-added, managed VPN services, such as multimedia applications, content delivery, IP telephony, e-commerce, and application hosting.

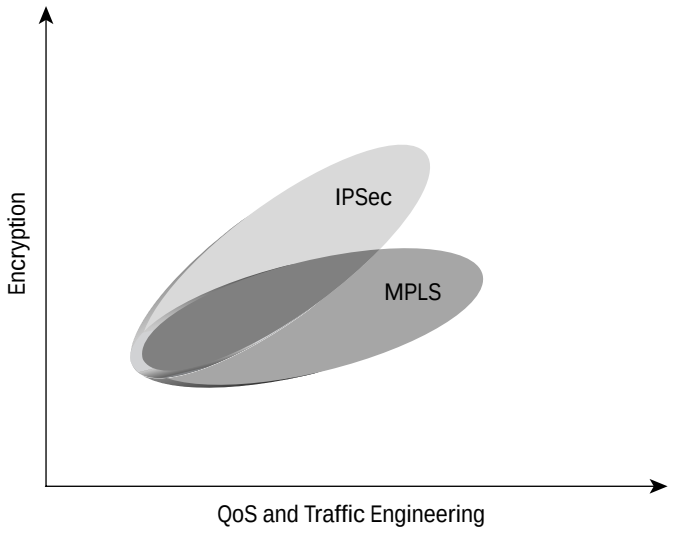
Cisco Managed IPSec CPE VPN Solution

The Cisco Site-to-Site IPSec VPN solution is a tested architecture that service providers can deploy rapidly to connect customer remote offices to enterprise networks. The connection is via an IPSec tunnel, either over the Internet or the service provider's IP network infrastructure. In either case, the service provider needs no network upgrades or changes to the network core. Cisco offers a broad set of platforms for the CPE, with optional hardware accelerators to improve encryption performance, and carrier-class management via the Cisco IP Solution Center. This solution enables service providers to provision VPNs in full-mesh, partial-mesh, or hub-and-spoke topologies. It supports IPSec as well as IPSec-over-GRE tunneling. The service provider can augment its VPN service by provisioning sub-topologies between CPE devices, each associated with a separate or consistent policy. The result is a seamless, end-to-end IPSec VPN service with integrated management.

Integrating IPSec with MPLS VPNs

MPLS and IPSec-based VPN are complementary rather than competitive. When used in combination, MPLS and IPSec can give service providers a competitive advantage. For example, service providers can use the IPSec-based VPN for off-net traffic that needs strong authentication and confidentiality, and link these VPNs directly to corresponding MPLS VPNs within the service provider core network to take advantage of their broader connectivity, traffic engineering, and QoS (see Figure 3).

Figure 3
Integrating IPSec and MPLS-Based VPNs



The Cisco Network-Based IPSec VPN solution enables service providers to map IPSec sessions directly into an applicable MPLS VPN (see Figure 4). Service providers can securely extend their VPN service beyond the boundaries of the MPLS network by using the Internet or partner networks. Business benefits to the service provider include the ability to offer VPN services that securely connect enterprise customers, their remote offices, telecommuters, and mobile users from anywhere to the corporate network. By extending the MPLS footprint into the Internet or partner networks, a service provider can offer its enterprise customers a more comprehensive portfolio of end-to-end VPN services. Centralized configuration and simplified network operations enable the service provider to serve more remote sites and enterprise users at a lower cost. The Cisco Network-Based IPSec VPN solution supports any combination of VPN deployment architectures (see Table 2).

Figure 4
Sample IPSec-to-MPLS Deployment Architecture

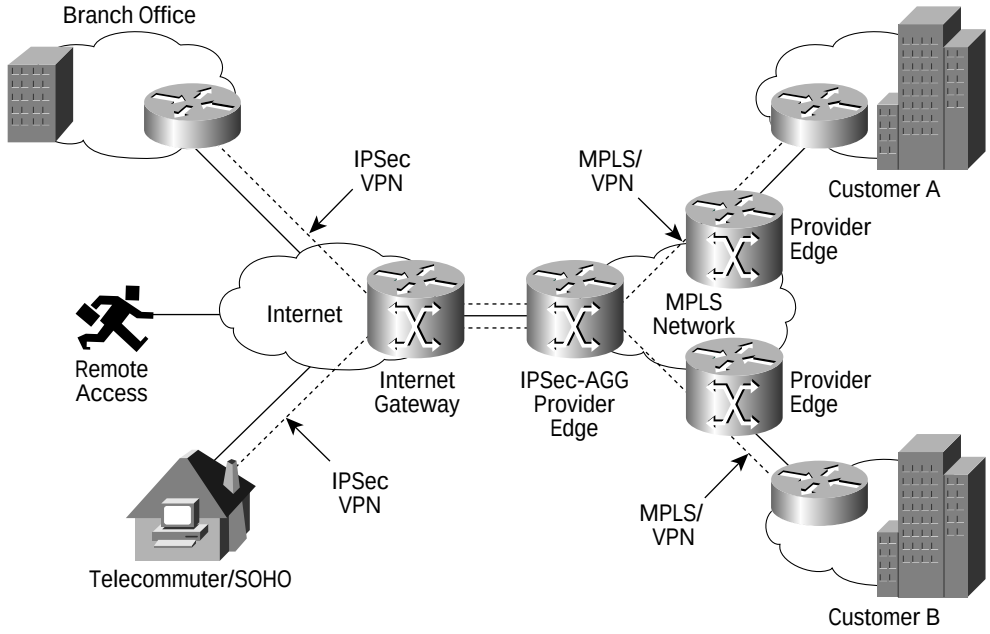


Table 2 The Cisco Network-Based IPSec VPN Solution Supports Any Combination of VPN Deployment

Deployment Architecture	Service Provider's Existing Network	Chief Capabilities
IPSec to MPLS	MPLS backbone	Enables secure off-net access to MPLS VPNs through IPSec Allows authenticated worldwide access via the Internet or partner networks
IPSec to Layer 2	Existing Layer 2 core: Frame Relay, ATM, 802.1q, or wireless	Allows extension of services, while still providing traffic separation for customers
IPSec to IPSec	Native IP or MPLS-enabled backbone	Allows operation with a device sized to support only a single IPSec tunnel rather than hundreds or thousands of IPSec tunnels Minimizes operational costs when the headend enterprise CPE platform is part of the service provider's managed service offering
IPSec to GRE	Existing IP backbone	Enables secure exchange of routing information across VPN sites
Provider edge to provider edge	Existing MPLS backbone	Encrypts traffic between provider-edge devices across network; eliminates the burden of enabling VPN on customer edge devices Maintains traffic separation provided by MPLS

Conclusion

Service providers can use network-based IP VPN services as a foundation for a value-added services portfolio. The choice of VPN architecture—MPLS-based, IPSec-based, or a combination—affects the service providers' potential service offerings, ease of management, security, and QoS, which are all factors that contribute to business customer service acceptance and service provider profitability.

Cisco Systems offers service providers a comprehensive choice of VPN infrastructure solutions, which integrate with a variety of existing network backbones and deliver various levels of high availability, scalability, security, QoS, and management. In general, MPLS VPNs are deployed in the service provider's core, and can also be used to create intranets or extranets for subscribers; IPSec VPNs are deployed at the local loop, edge, and off-net, where security is most crucial. Many service providers can benefit from the combination of MPLS and IPSec found in the Cisco Network-Based IPSec VPN solution. By blending the technologies, service providers can take advantage of the strong confidentiality and authentication of IPSec for off-net traffic, and the greater connectivity, traffic engineering, and QoS of MPLS within the core network. By taking advantage of the respective strengths of MPLS and IPSec, the service provider can expand its service portfolio, maximize its potential customer base, and ultimately gain a competitive advantage.

For more information about Cisco IP VPN infrastructure solutions, visit:

http://www.cisco.com/go/vpnsolutions

To view an e-tour of managed services, visit:

http://www.cisco.com/go/managedservicesetour

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

N2/KW/LW5590 1/04