White Paper

Virtual Private Network Architectures—Comparing Multiprotocol Label Switching, IPSec, and a Combined Approach

Introduction

In the present economy, service provider profitability hinges on moving beyond a focus on transport to delivering value-added services. The market for managed virtual private network (VPN) services is expected to reach $5.3 billion by 2006, according to research firms IDC and Ovum. Managed VPN services can include e-commerce, IP telephony, managed security, remote site backup, application hosting, and multimedia applications. The type and deployment of a VPN architecture—Multiprotocol Label Switching (MPLS), IP Security (IPSec), or a combination of these—influence the service provider's market coverage, service offerings, and revenue.

This white paper compares MPLS- and IPSec-based VPN architectures. It begins by explaining the evolution of the two distinct VPN technologies, and the general goals for VPN architectures. Next, it presents the relative strengths of MPLS- and IPSec-based VPNs and explains where service providers can deploy each architecture for optimum advantage. The white paper concludes with a brief description of the integrated IPSec-to-MPLS VPN solution from Cisco Systems, which takes advantage of the respective strengths of the two architectures.

Why Two VPN Architectures?

In recent years, two Internet Engineering Task Force (IETF) working groups have been established, focusing on three important components of VPNs—Internet security, label switching standardization, and quality of service (QoS). In the IETF's Routing Area, the MPLS working group is developing mechanisms to support higher-layer resource reservation, QoS, and definition of host behaviors. Concurrently, in the IETF's Security Area, the IPSec working group is concentrating on the protection of the network layer by designing cryptographic security mechanisms that can flexibly support combinations of authentication, integrity, access control, and confidentiality. The IETF has left the issue of integrating MPLS and IPSec to the discretion of networking vendors. As a result, two VPN architectures have emerged—one based heavily on MPLS and the other on IPSec.

MPLS and IPSec-based VPNs are complementary rather than mutually exclusive. Service providers can increase their service footprint and gain other competitive advantages by using the strengths of the two architectures.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Essential Attributes of VPNs

The service goal of VPNs is to provide customer connectivity over a shared infrastructure, with the same policies enjoyed in a private network. A VPN solution must protect against intrusion and tampering, deliver mission-critical data in a reliable and timely manner, and be manageable. Following are essential attributes of VPN architectures.

Scalability

A service provider's VPN deployments might range from small office configurations through the largest enterprise implementations, spread across the globe. The VPN architecture must adapt to meet customers' ever-changing bandwidth and connectivity needs. 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 unplanned growth and changes driven by customer demand. Service providers that have the potential to support tens of thousands of VPNs over the same network maximize their revenue and profit potential.

Security

It is essential that the VPN protect sensitive data so that it remains confidential. Security mechanisms used in VPNs include tunneling, encryption, traffic separation, packet authentication, user authentication, and access control.

QoS

Support for QoS enables the VPN to prioritize mission-critical or delay-sensitive traffic such as voice and video, and also to manage congestion across varying bandwidth rates. QoS mechanisms include queuing, network congestion avoidance, traffic shaping, and packet classification.

Manageability

Typical VPN management tasks include:

- Provisioning
- Distributing and installing VPN-enabled customer premises equipment (CPE) and VPN software clients where needed
- Installing security and QoS policies
- Managing and making changes to VPNs
- Billing
- Supporting service-level agreements (SLAs)

To perform these tasks, the service provider relies on an operations support system (OSS). An OSS with automated flow-through provisioning systems, reporting, and monitoring enables service providers to quickly fulfill VPN orders and support SLAs.

Reliability and Redundancy

The VPN must be able to deliver the predictable and high service availability that business customers expect and require. A combination of reliability and redundancy is the key to maintaining business continuity and recovering from failures. Mechanisms to improve service availability include enabling the VPN network to provide server stateful failover, VPN redirect, VPN session keepalive, VPN redundant server and backup sites. Some of these mechanisms may be offered by the service provider as a premium service at additional cost.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

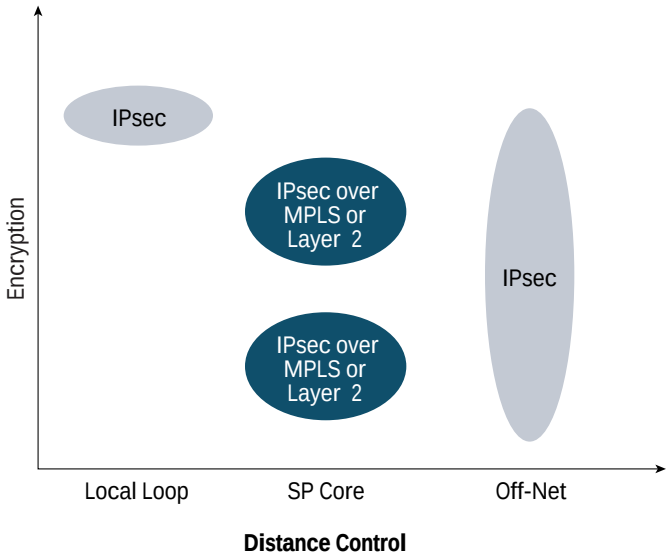
The Role of MPLS

MPLS fuses the intelligence of routing with the performance of switching. It provides significant benefits to networks with a pure IP architecture, those with combined IP and ATM, and those with a mix of other Layer 2 technologies. MPLS technology is a key enabler of scalable VPNs, making it easy for service providers to efficiently use their existing networks to meet future growth. Its end-to-end QoS enables rapid fault correction of link and node failure. MPLS also helps deliver highly scalable, differentiated end-to-end IP services with simpler configuration, management, and provisioning.

MPLS is primarily deployed in the core of a service provider's network (Figure 1). It enables routers at the edge of a network to apply simple labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels, with minimal lookup overhead. MPLS integrates the performance and traffic management capabilities of data link Layer 2 with the scalability and flexibility of network Layer 3.

MPLS can be implemented on networks based on IP, ATM, and Frame Relay. Thus, for carriers with existing autonomous ATM and Frame Relay infrastructures—including many incumbent local exchange carriers (ILECs); post, telegraph, and telephone (PTT) companies; and interexchange carriers (IXCs)—MPLS creates a migration path to a more efficient and flexible IP-based converged infrastructure.

Figure 1
Network Location for MPLS and IPSec



MPLS Strengths

Following are key 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. The scalability is inherent because there is no need for site-to-site peering.
- *Security*—MPLS keeps each VPN's traffic separate by using unique route distinguishers. Assigned automatically when the VPN is provisioned, route distinguishers are placed in packet headers as a mechanism to provide traffic separation, and are transparent to end users within the VPN group.
- *Traffic engineering*—Traffic engineering is enabled through MPLS mechanisms that allow traffic to be directed through a specific path (not necessarily the least expensive path). By using traffic engineering in the core, network engineers can implement policies to ensure optimal traffic distribution and improve overall network use.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- *Class of service (CoS)*—The CoS features in MPLS enable service providers to provide differentiated types of services across the MPLS network, simply by marking packets with a differentiated services code point (DSCP) and treating them accordingly. Techniques used to support differentiated services include packet classifications, congestion avoidance, and management
- *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.

Cisco MPLS-Based VPN Solution

The basic architecture for the Cisco MPLS-based VPN solution can consist of:

- Cisco IOS® Software-based routers, from the Cisco 3600 Series through Cisco 12000 Series Internet routers
- Cisco MGX® 8850 IP+ATM multiservice switches
- Cisco VPN Solution Center (VPNSC), a centralized network management platform typically managed at the service provider network operations center (NOC)

The Role of IPSec

Based on open standards developed by the IETF, IPSec ensures confidentiality, integrity, and authenticity of data communications across the public Internet. IPSec contributes a necessary component of a standards-based, flexible solution for deploying a network-wide security policy.

IPSec functions at the network layer (Figure 1). It is most useful at the local loop, the edge, and outside of a service provider's network (off-net), where there is a higher degree of exposure to breaches of data privacy and where IPSec security mechanisms such as tunneling and encryption can best be applied. IPSec is especially useful for securing remote-access VPN connections back to the corporate network.

IPSec Strengths

Following are key strengths of IPSec-based VPNs:

- *Security*—IPSec ensures 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. It can be deployed across any existing IP network.

Cisco IPSec-Based Solution

The Cisco Managed IPSec VPN solution consists of a combination of the following elements:

- Cisco 800, 1700, 2600, 3600, 7100, 7200, and 7400 series VPN-enabled routers
- Cisco PIX® 500 Series Firewall
- Cisco VPN 3000 Series Concentrator
- VPN acceleration modules (VAMs) for Cisco 7100 and 7200 Series routers, which provide high-performance, hardware-assisted encryption, key generation, and compression services for VPN applications
- Cisco VPN Solution Center (VPNSC)

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Table 1 below compares MPLS-Based VPNs to IPSec VPNs in terms of several key attributes including scalability, security, QoS, and provisioning.

Table 1 Comparing MPLS- and IPSec-Based VPNs

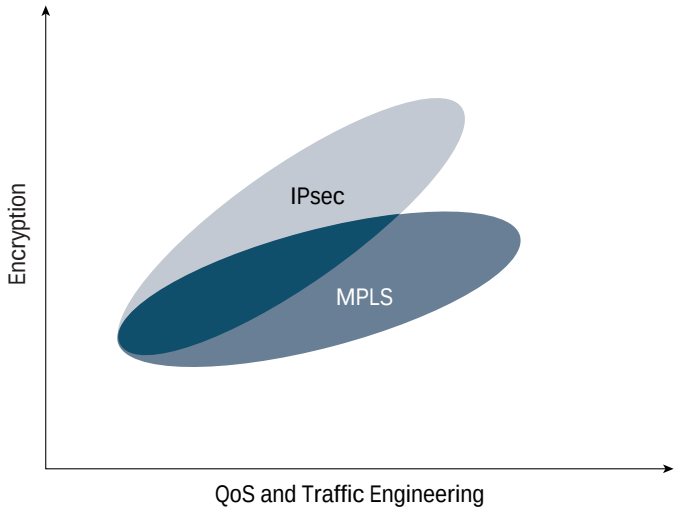
	MPLS-Based VPN	IPSec-Based VPN
Service models	• High-speed Internet services • Business-quality IP VPN services • E-commerce • Application-hosting services • Managed security • Managed IP telephony • Remote site backup	• High-speed Internet services • Business-quality IP VPN services • E-commerce • Application-hosting services • Managed security • Managed IP telephony • Remote site backup
Scalability	• Highly scalable—no site-to-site peering is required • Capable of supporting tens of thousands VPNs over the same network	• A very large IPSec-based VPN deployment 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
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
Provisioning	• One-time provisioning of customer-edge and provider-edge devices to enable the site to become a member of an MPLS VPN group	• In general, no network-level provisioning is required for CPE-based service offering • Centralized provisioning for network-based service offering
Service deployment	• Participating network elements at the core and edge must be MPLS-capable	• Fast time to market • Can be deployed across any existing IP networks
Session authentication	• VPN membership established during provisioning, based on logical port and unique route descriptor • Access to a VPN service group is defined during service configuration; unauthorized access is denied	• Via digital certificate or preshared key • Packets that do not conform to the security policy are dropped
Confidentiality	• Achieved via traffic separation, similar to technique used in trusted Frame Relay or ATM network environments	• Via a flexible suite of encryption and tunneling mechanisms at the IP network layer
QoS and SLAs	• Achieved via scalable, robust QoS mechanism and traffic engineering capability	• Not addressed directly by IPSec • Cisco IPSec VPN deployments can preserve packet classification for QoS within an IPSec tunnel
Client support	• Not applicable; MPLS VPN is a network-based VPN service	• IPSec VPN deployments • Cisco VPN client software is available for Microsoft Windows as well as operating systems such as Solaris, Linux, and Mac OS
User interaction	• No user interaction required	• For client-initiated IPSec VPN service offering, users need to interact with the IPSec client software

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Integrating IPSec with MPLS VPNs

Service providers can achieve the greatest benefit by applying both IPSec and MPLS technology. For example, service providers can use IPSec for off-net traffic that needs strong authentication and confidentiality, and use MPLS at the network core for its broader connectivity, traffic engineering, and QoS (Figure 2).

Figure 2
Integrating IPSec and MPLS

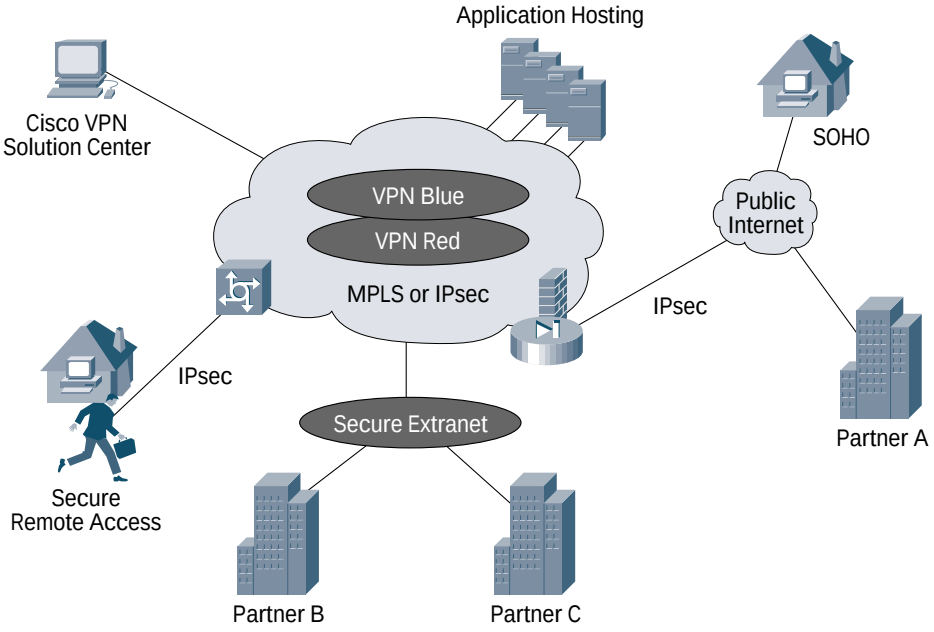


Cisco offers a solution that enables service providers to map IPSec sessions directly into an MPLS VPN. The solution is deployed on colocated edge routers that are connected to a Cisco IOS Software MPLS provider-edge network, which can include Cisco 7200, 7500, MGX 8800, 10000, or 12000 Series routers. This approach enables the service provider to securely extend its VPN service beyond the boundaries of the MPLS network by using the public IP infrastructure (Figure 3). The service provider can 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.

The Cisco VPNSC efficiently manages all components of the integrated IPSec-to-MPLS VPN, simplifying provisioning and management.

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Figure 3
Integrated IPSec-to-MPLS-Based VPN Network



Conclusion

VPNs address a key need in the present telecommunications market—supplementing existing revenue streams with new, profitable, value-added services. The choice of VPN architecture affects the service provider's potential service offerings, ease of management, security, and QoS—all factors that contribute to service acceptance and profitability.

Cisco MPLS-based VPN solutions deliver the broadest connectivity, overall cost efficiency, and a migration path for legacy Frame Relay and ATM networks. Cisco IPSec-based VPN solutions, in turn, deliver strong authentication and confidentiality. With an integrated IPSec-to-MPLS VPN solution, service providers can reap the benefits of both technologies, gaining optimum security and QoS as well as the scalability and flexibility to meet the varying and ever-changing requirement demands of their customers.

For more information, visit: http://www.cisco.com/go/vpnsolutions.

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 Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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: +65 317 7777
Fax: +65 317 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

All contents are Copyright © 1992–2003, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, MGX, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

DH/CI/0703