



SERVICE OVERVIEW

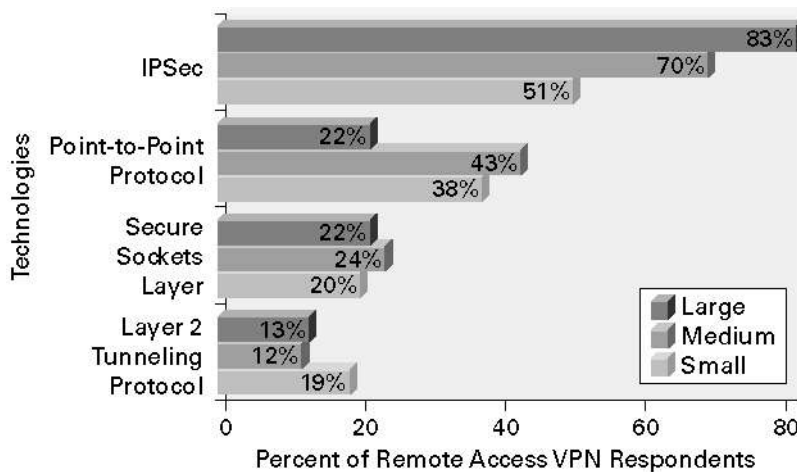
MANAGED IPSEC-BASED VPN SERVICES

For businesses of all types and sizes, a secure and well-managed corporate network is an important means to support business operations and enable increased growth, productivity, and profitability. VPNs based on the IP Security (IPSec) protocol have become a cost-effective, scalable alternative for enterprises that need a secure, economical, and simple way to connect remote sites, employees, and business partners to networked systems and applications.

IPSec offers the security and encryption features necessary to protect enterprise data, IP voice, and video traffic as it traverses the Internet or a service provider's shared network. Because this protocol can be deployed across any IP network, IPSec is an attractive option to service providers for delivering VPN services.

For a service provider, IPSec functions well end to end, at the network edge, and within the core network. This design makes IPSec an excellent solution for site-to-site as well as "on-net" (over the service provider's shared networks) and "off-net" (over the Internet or a partner's network) remote-access implementations to meet different customer needs. For example, as the number of geographically dispersed mobile users and remote offices increases, secure off-net VPN connectivity will become an increasingly important offering for service providers. Infonetics, a leading market-research company, conducted a survey to determine business plans for supporting remote users. In the survey results, IPSec shows stronger adoption by all business segments in the U.S. market compared to all other non-network-based VPN tunneling protocols (Figure 1).

Figure 1
VPN Tunneling Protocol Adoption by Market Segments



Source: Infonetics, 2002

By operating at the IP layer, IPSec offers the service provider greater choice for the underlying network structure, enabling a wide range of services and accelerating the time to market. In an IPSec-based VPN, application modifications are not required, and there is no need to deploy and coordinate security on a per-application, per-computer basis. IPSec provides a secure VPN technology without costly changes to every computer on the network—an important and highly attractive benefit to enterprises.

Managed IPSec VPNs also provide a foundation for service providers to offer business customers additional services that require secure connectivity such as IP telephony, videoconferencing, e-commerce, and application hosting.

This document gives service providers insights into the market potential for IPSec VPNs and the Cisco Systems® solutions for creating optimal IPSec VPN service offerings.

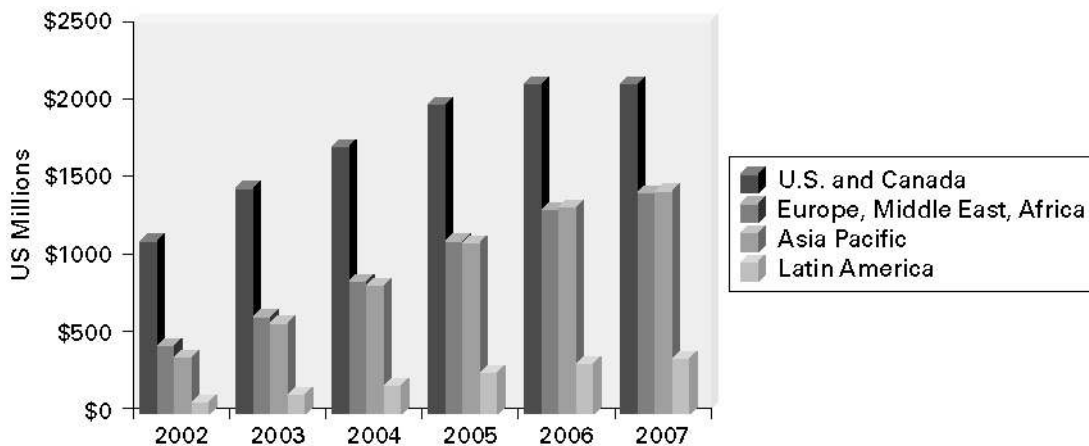
MANAGED IPSEC VPN MARKET OPPORTUNITY

Enterprises can gain many benefits from managed IPSec VPN services, including expanded market reach, improved employee productivity, reduced operational expenses, and enhanced security. Service providers can attract enterprise customers by demonstrating how an out-tasked VPN service delivers these benefits.

According to market-research company Ovum, the adoption rate for IPSec is strong across all world regions but especially in the United States. For IPSec site-to-site VPN services, projected revenue in the United States and Canada is expected to increase from US\$1.5 billion in 2003 to more than US\$2.1 billion in 2006 (Figure 2). As this chart shows, forecasted growth rates are also strong for Asia Pacific and European countries.

Figure 2

Projected IPSec Site-to-Site VPN Service Revenue by Regions



Source: Ovum, July 2003

Market Segmentation

This paper segments the IPSec VPN services market according to company size, a factor that differentiates service requirements and opportunities.

Large enterprises (1000 or more employees) view IPSec VPNs as extensions to existing network infrastructures. To meet these customers' requirements for authenticated and secure access to corporate applications, IPSec VPN services must support strong security and compatibility with existing network designs while ensuring ongoing cost savings and scalability.

Midsized businesses (100 to 1000 employees) want IPSec VPNs to deliver secure remote access for mobile workers and telecommuters who increasingly use the Internet for connectivity to company network resources. Quality of service (QoS) for traffic prioritization, the ability to add new users quickly, and ease of management are also important criteria for midsized businesses in choosing IPSec VPN services.

Small businesses (20 to 100 employees) are extremely price-sensitive, are interested in outsourcing because they often lack in-house expertise, and prefer bundled solutions. IPSec VPN services for these businesses must offer reduced costs for network access, equipment, and maintenance as well as simplified management of remote sites and users.

Market Influences

The market for managed IPSec VPN services is distinguished specifically by high requirements for network security and data privacy. The demand for managed IPSec VPNs continues to grow because of several market influences such as:

- **Security**—Enterprise customers understand the need to protect networks, systems, applications, and data from security breaches and risks that come with connection to shared networks. However, not all businesses have the internal resources and knowledge necessary to proactively monitor, manage, and keep current with the latest security advances to deter and mitigate network attacks. These customers want to take advantage of secure VPN services as well as a service provider's expertise and resources for managing overall network security.
- **IPSec advancements**—IPSec is a highly secure infrastructure to transport proprietary information over the public Internet and other shared networks. IPSec provides data privacy through a flexible suite of encryption and tunneling mechanisms that protect packet payloads as they traverse a public network. IPSec can also protect traffic in a service provider's core network and especially at the network edge, where there is a higher degree of exposure to data privacy risks.
- **Remote-access demand**—Continued growth in the number of geographically dispersed teleworkers and mobile users means businesses need service providers to offer remote network access from any location. These connections can be made directly to a headquarters site via an on-net service, or indirectly through an off-net service to the provider's nearest point of presence (POP) via the Internet or a partner's network.
- **Technology**—IP is fast replacing Frame Relay and ATM as the foundation for enterprise networks because IP offers advantages for security, QoS, performance, and communications convergence.
- **Regulatory**—The need for network security is also driven by legislation to ensure consumer privacy for all forms of electronic data and communications, especially over the Internet. For example, in the United States, healthcare and financial enterprises must meet federal mandates for data privacy and security and ensure compliance by vendors and business partners as well. Many other countries also have strict rules governing data privacy on enterprise networks.

MANAGED IPSEC VPN SERVICE DESCRIPTION

An IPSec VPN enables mobile workers and geographically dispersed remote branch offices to cost-effectively and securely connect to enterprise intranets or extranets using the service provider's shared IP networks, a partner's network, or the Internet. Although the connection is made over a shared network, an IPSec VPN can have the same management and security policies as a private network.

IPSec VPNs can be delivered in the following ways:

- As a site-to-site VPN through customer premises equipment (CPE) that supports IPSec
- As a network-based VPN delivered directly from the service provider's network
- As an on-net remote access VPN with all connections made through the service provider's own network
- As an off-net remote access VPN with connections made via the networks of other service providers or over the Internet
- As a VPN extension for a customer's existing Frame Relay and ATM network

Site-to-site IPSec VPN services overlay Layer 3-encrypted tunnel connections on the shared network in a hub-and-spoke, full-mesh, or partial-mesh design. A CPE-based implementation of this architecture requires a security appliance such as an IPSec-enabled router or firewall at each customer site. As a managed service, the service provider supplies and manages the CPE and configures the associated VPN connection.

In contrast, a network-based IPSec VPN architecture enables service providers to:

- Support and manage large enterprise deployments, overcoming the limits to scalability inherent in a CPE-based VPN architecture.
- Securely interconnect customer sites between provider edges across the network core in order to deliver secure on-net and off-net remote VPN access through IPSec tunnels. This security is possible because a network-based IPSec VPN originates and terminates in the service provider network.
- Reduce costs and operational demands because there is little need for provisioning individual customer devices when VPN services are delivered directly from the network.
- Offer an expanded VPN service portfolio that includes full integration of remote access VPNs with site-to-site VPNs as well as service options such as QoS priorities and service-level agreements (SLAs).

IPSec VPN Service Features

Service providers can offer a variety of basic features as part of an IPSec VPN service, such as those listed in Table 1.

Table 1. Potential Features for a Managed IPSec VPN Service

Category	Features
Security	Encryption, security features, and network monitoring protect data from tampering or exposure when it is transported over the shared network and protects a customer's internal networks by permitting only authenticated access.
Choice of access speeds and connectivity options	Support for a range of access speeds, from fractional T1 through DS-3 and including broadband cable, DSL, and wireless technologies.
Flexible pricing schemes	Enterprise customers will expect multiple options, from fixed prices based on the access bandwidth and services selected to usage-based pricing.
Service provisioning and device management	As part of a managed service offering, the service provider will provision and manage the network connections and CPE such as VPN-enabled routers, firewalls, and authentication, authorization, and accounting (AAA) servers. A service provider may also offer options such as QoS priorities and SLAs, equipment replacement or repair, and coordination with third-party vendors.
Support for new applications	Multicast features maximize efficiency for secure videoconferencing, e-learning, and other high-bandwidth applications with simultaneous connectivity to multiple sites.

CISCO IPSEC VPN SOLUTIONS

As a networking vendor, Cisco® is uniquely positioned to help service providers create new revenue opportunities by using IPSec for VPN services, whether network-based or CPE-based, in site-to-site or remote-access deployments. Cisco VPN solutions—routing platforms, security features, network services, VPN-enabled devices, and management tools—allow service providers to offer businesses of all sizes a broad range of VPN services.

Cisco Network-Based IPsec VPN Solution

The Cisco Network-Based IPsec VPN solution enables centrally managed, end-to-end secure VPN connectivity for on-net and off-net remote access and site-to-site VPN services. This solution supports the following VPN deployment architectures:

- IPsec to Multiprotocol Label Switching (MPLS)
- IPsec to Layer 2 using Layer 3 routing
- IPsec to IPsec
- IPsec to generic routing encapsulation (GRE)
- Provider edge-to-provider edge encryption

Cisco Site-to-Site CPE-Based IPsec VPN Solution

The Cisco Site-to-Site CPE-Based IPsec VPN solution gives service providers a tested architecture that can be deployed immediately to connect remote offices to enterprise networks using IPsec tunnels. This architecture supports VPN services that run over the Internet or a service provider's core network.

The scalable Cisco Site-to-Site CPE-Based IPsec VPN solution is suitable for enterprise data centers, regional and remote offices, and small office or home office (SOHO) locations, supporting a broad range of access technologies. Cisco offers a broad set of platforms for the CPE, with optional hardware accelerators to improve encryption performance. These solutions give service providers an end-to-end IPsec VPN service with integrated device management for improved time to market.

Service Provider Success Story

Belgacom, the incumbent service provider in Belgium, is already realizing the business advantages of offering IPsec VPN services. Belgacom has implemented the Cisco Network-Based IPsec VPN solution on an MPLS-enabled network. This solution enables Belgacom to offer secure remote connectivity over DSL lines for both enterprise and small and midsize business (SMB) customers through the company's e-Link service. By deploying the Cisco IPsec VPN solution, Belgacom can offer new services to the new SMB market segment and gain additional revenue from its existing MPLS infrastructure with only a small additional investment.

FOR MORE INFORMATION

A more detailed discussion of the topics in this document is presented in the white paper *Implementing Managed IP Virtual Private Network Services*, available at: <http://www.cisco.com/go/vpnservices>

To view an informative E-Tour about opportunities for managed VPN services, visit: <http://www.cisco.com/go/managedservicesetour>

To learn more about Cisco solutions for IPsec VPNs, contact your Cisco account manager or 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 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.
168 Robinson Road
#28-01 Capital Tower
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 Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • 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



Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0406R)

He/LW7489 12/04