

Cisco Network-Based IPsec VPN Solution

Q. What is the Cisco® Network-Based IPsec VPN solution?

A. The Cisco Network-Based IPsec VPN solution enables a service provider to offer scalable, turn-key services to securely connect both remote users and remote sites to a customer's corporate VPN network. Through the integration of IPsec into an MPLS, IP, or Layer 2-based VPN service offering, service providers can extend their network to include remote locations that need to be serviced over a public IP infrastructure. By extending the VPN footprint over the Internet or partner networks, a service provider can offer a more comprehensive bundle of end-to-end VPN services to its enterprise customers.

Q. What companies will benefit most from this solution?

A. The primary market for this solution includes service providers with the following attributes:

- Currently offer MPLS VPN services and want to extend their geographic coverage without building out their network
- Are focused on capturing the mobile worker and telecommuter VPN customers without building out their network

The secondary market for this solution includes service providers with one or more of the following attributes:

- Operate an IP core or plan to deploy an IP core and offer VPN services over that
- Offer an existing Layer 2 Frame Relay or ATM service and want to extend geographic coverage
- Currently offer or plan to offer broadband aggregation services and plan to offer VPN services
- Are a mobile/wireless operator that wants to backhaul traffic over the Internet
- Offer hosting services and want to offer secure access as a premium service

Q. How can this solution help service providers in today's economic climate?

A. This new Cisco solution enables service providers to take full advantage of their existing network investment and

- Generate new revenue streams
- Increase service differentiation
- Improve customer satisfaction
- Maximize return on existing or new investment



Supported by the Cisco 7200 Series platform at the provider edge, service providers currently offering MPLS VPN services can quickly and easily introduce this new network-based IPsec VPN service to meet enterprise customer requirements for secure, ubiquitous connectivity from remote locations to the corporate network.

Q. What key benefits do service providers derive from the solution?

A. The Cisco Network-based IPsec VPN solution enables a service provider to offer a cost-effective and scalable encrypted VPN service to customers that require highly secure access into their corporate networks.

By deploying this Cisco solution, a service provider can:

- Expand its VPN service portfolio and generate incremental VPN revenue
- Deliver fully integrated remote access VPNs to expand geographic coverage
- Use existing infrastructure and improve economy of scale of the network by supporting multiple customer VPNs on a single network edge platform
- Offer a wider distribution of products and services to suit enterprise and small and medium-sized business (SMB) customer requirements
- Reduce overall network management operations and costs by centralizing the provisioning of services and customer premises equipment (CPE)

Q. Who are the targeted enterprise customers for this solution?

A. Target customers include enterprises and SMBs with geographically dispersed branch offices and a significant telecommuter/mobile workforce. In some cases, these customers are already receiving an MPLS VPN service from a service provider and wish to outsource all of their VPN services to the same provider.

Q. How do enterprise and SMB customers benefit from this solution?

A. This solution enables service providers to offer companies of all sizes, a managed, scalable IPsec VPN connection to access corporate resources remotely. Benefits for the enterprise and SMB customers include:

- Ability to outsource the management of transport, equipment, and secure VPN access to the service provider at a predictable fixed cost
- Reductions in service downtime
- Reduction in networking capital expenditures
- Ability to focus on the core business
- Ability to expand market presence without compromising on connectivity and associated productivity
- Ability to reach more customers, partners, distributors, and suppliers through the Internet
- Improved employee productivity

Q. What are the key features of this solution?

A. The key features of the solution include:

- *Virtual route forwarding (VRF)-aware Internet Key Exchange (IKE)/IPsec*—This feature enables the service provider to support multiple customer VPNs on a single edge platform.

This feature provides the ability to dynamically add new customers without adding interfaces or redesigning IP addressing schemes on the edge platform, using a single public-facing interface.



- *Per-VRF authentication, authorization, and accounting (AAA) function*—Support for flexible authentication and authorization architectures using either the service provider’s AAA server or the customer’s AAA server. Also, VRF-aware IPsec accounting enables billing support on a per-VPN basis.
- *Scalability and redundancy*—Support for multiple IPsec network edge platforms as a single logical entity using server load balancing on a Cisco Catalyst® 6500 Series switch.
- *Stateless failover*—When the primary network edge platform fails, IPsec sessions can failover and reconnect to the backup network edge platform, thus minimizing connection downtime.
- *Easy VPN Client support*—Cisco IOS® Software supports the Cisco UnitySM VPN Client function on the low-end router platforms. This enables the service provider to push IPsec policies onto CPE, thereby minimizing the configuration tasks on these routers. The solution also supports software VPN clients for the Windows, Macintosh, Solaris, and Linux platforms.
- *Network Address Translation (NAT) transparency*—IPsec sessions are successfully negotiated even if they have traversed through a NAT device in the network before reaching the network edge.
- *Site-to-site support*—Support for LAN-to-LAN tunnels with or without generic route encapsulation (GRE) tunnels for CPE-to-CPE connectivity. GRE tunnels can be used to carry dynamic routing protocols to transparently integrate customer VPN sites.

Q. How is this solution managed?

A. The Cisco Network-Based IPsec VPN solution can be provisioned using the Cisco IP Solution Center 3.0. Some of the salient features of Cisco IP Solution Center 3.0 include:

- Provisions both the MPLS VPN and the IPsec VPN connection to the CPE devices from the network edge
- Uses a highly distributed architecture that can scale to a large number of connections and the internal database maintains all the information on the IPsec connections and their association with the relevant MPLS VPN
- Supports a browser-based graphical user interface (GUI)
- Supports different user profiles with access control privileges to provide different views of the network based on the profile
- Configures the Service Assurance Agent (SAA) on the Cisco routers to generate service-level agreement (SLA) reports
- Passes IPsec-specific Management Information Base (MIB) and trap information, available on Cisco routers, to third-party operations support system (OSS) applications for fault management and performance management

Q. How does this solution lower total cost of ownership in both operating and capital expenses (OpEx and CapEx)?

A. By moving VPN services to the network edge where cost control and scalability can be enhanced, providers aim to capture the majority of dollars spent on security services at a point that yields the highest rate of return. Service providers can centralize configurations and streamline overall network maintenance operations, control their costs, and improve the economy of scale of the network, thereby reducing OpEx and CapEx. For more information about reducing expenses, please ask your account executive about the business case and the related VPN Payback Tool for the Cisco Network-Based IPsec VPN solution.

Q. When is the solution available and which Cisco IOS Software release supports it?

A. Phase 1.5 of the solution has been available since March 17, 2003. This phase of the solution is supported on Cisco IOS Software Release 12.2(15)T.

Q. What are the key components of this solution?

A. This solution consists of the following:

- *IPsec aggregation device:*

The Cisco 7204 and 7206 routers serve as IPsec aggregation devices. They support the NPE-400 and NPE-G1 processors and the VPN accelerator modules (VAMs).

- *CPE devices:*

Cisco PIX[®] Firewall, Cisco VPN 3002 Hardware Client, Cisco 800 Series routers, Cisco 1700 Series routers, Cisco 2600 Series routers, Cisco 3600 Series routers, and Cisco 7200 Series routers.

- *VPN clients:*

The Cisco VPN Client with support for the following operating systems: Microsoft Windows, Linux, Sun Solaris, and the Apple Mac OS.

Easy VPN Client support on Cisco IOS Software-based CPE devices.

- *Provisioning and network management:*

Cisco IP Solution Center 3.0 provides scalable MPLS VPN and IPsec VPN provisioning capability and network management support.

- *Cisco IOS Software:*

Cisco IOS Software Release 12.2(15)T or later.

Q. Where can I get more information?

A. The solution has an extensive set of technical documents:

- Technical Solution Overview
- Release Notes
- Overview and Planning Guide
- Operations, Maintenance, and Troubleshooting Guide

Visit the Solution Portal at:

<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.
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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco Unity is a service mark of Cisco Systems, Inc.; and Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, 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) SP/LW4584 05/03