Whitepaper

Cisco VPN Solution Center 2.2

Introduction

The Cisco VPN Solution Center 2.2 (VPNSC 2.2) is a carrier-class network- and service-management solution for the rapid and cost-effective delivery of IP virtual private network (VPN) services. VPN services based on Internet Protocol (IP) and targeted to enterprise customers can represent major revenue opportunities for service providers. Success in this highly competitive market requires the ability to effectively plan, provision, operate, and bill for IP VPN services.

The Cisco VPN Solution Center offers both Multiprotocol Label Switching (MPLS) and Security (IPSec) IP VPN service providers a customizable service- and network-management solution to facilitate successful, profitable, and rapid VPN service deployment. For service providers using the IPSec or MPLS transport framework, the Cisco VPN Solution Center provides a full complement of provisioning, monitoring, and administration tools that simplify the inherent complexities of managing a VPN infrastructure. By streamlining virtually every process in the VPN life cycle, Cisco VPN Solution Center helps service providers quickly and cost-effectively meet evolving customer requirements for functionality, security, and quality of service (QoS).

Cisco VPN Solution Center 2.2: MPLS Solution

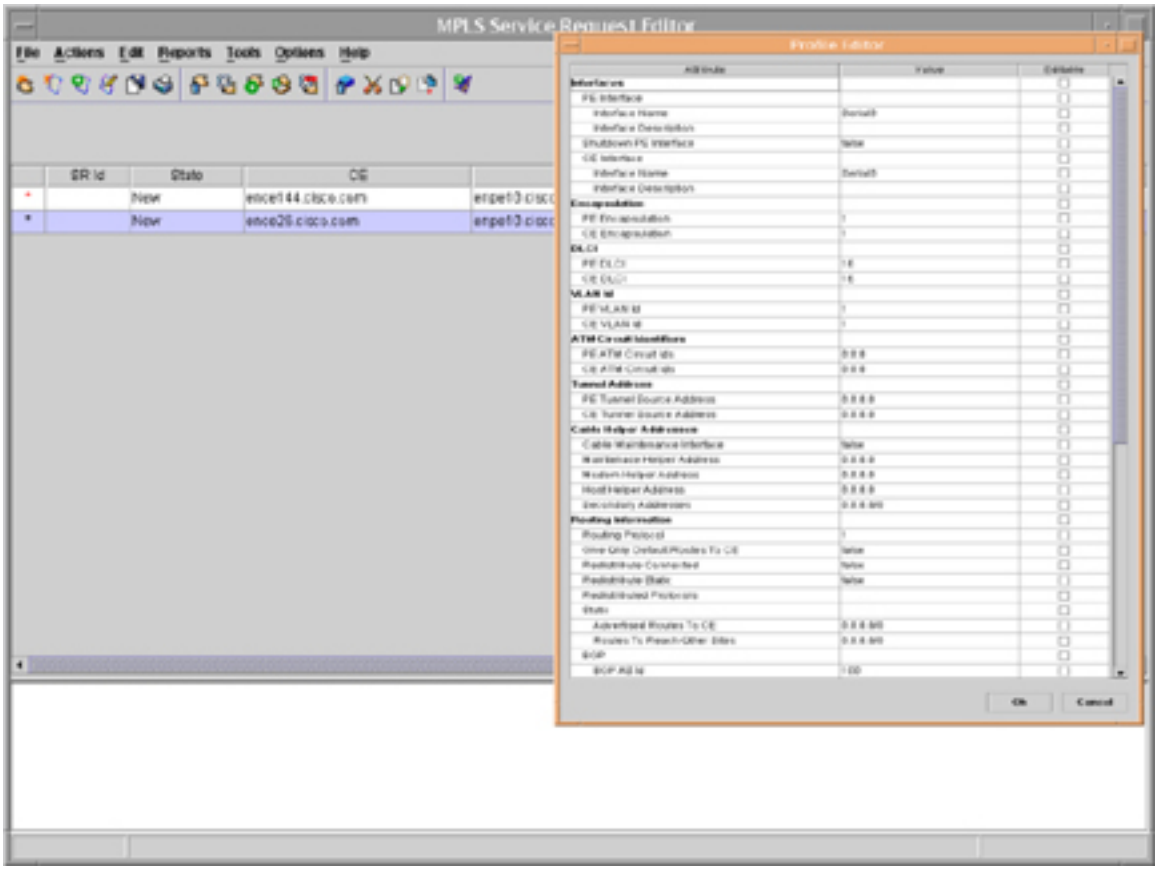
Cisco VPN Solution Center 2.2 provides management of IP VPN services throughout the service life cycle including service provisioning and activation on customer-edge and provider-edge routers, service auditing and service-level agreement (SLA). The set of well-defined Common Object Request Broker Architecture application programming interfaces (CORBA APIs) provide external operations support systems (OSSs) access to the full capability of the Cisco VPN Solution Center, allowing flow-through provisioning and SLA monitoring.

The Cisco VPN Solution Center complements Cisco VPN solutions by simplifying the planning, provisioning, and service-assurance processes, thereby reducing the cost of deploying and operating VPN services. Operators and upstream systems can add, delete, or modify customer MPLS VPNs and define the associated VPN service topology (hub-and-spoke, full, and extranet) via Cisco VPN Solution Center user interface or APIs. Wizards assist service technicians by simplifying the process of entering requested VPN service-related information, including customer and SLA profiles and QoS parameters for the service. The software then translates the VPN service request information into configurations

that implement the VPN service and validates the configuration. The Cisco VPN Solution Center keeps track of the current VPN state, including error conditions, of the service request and scheduled tasks.

Cisco VPN Solution Center also supports router console provisioning and templates to allow operators to stage customer-edge devices in a managed service environment. Cisco VPN Solution Center can be used to activate Layer 3 configuration of the VPN service from initial router configuration to VPN service activation. Figure 1 depicts the MPLS module of the Cisco VPN Solution Center.

Figure 1
Cisco VPN Solution Center 2.2: MPLS Solution



Cisco VPN Solution Center 2.2: Security (IPSec) Solution

The Cisco VPN Solution Center 2.2 security module enables customers to efficiently manage IPSec VPN deployment by configuring Internet Key Exchange (IKE) and IPSec tunnels between routers based on Cisco IOS® Software, Cisco VPN 3000 Series concentrators, or Cisco PIX® Firewall devices automatically with just minimum high-level service input from the users. Automating otherwise time-consuming and complex tasks—including resolving incompatible or inconsistent IPSec and IKE policies among devices and the routing protocols among sites—that only worsen as the VPN scales in size. The Cisco VPN Solution Center helps customers more rapidly respond to expanding and evolving client requirements.

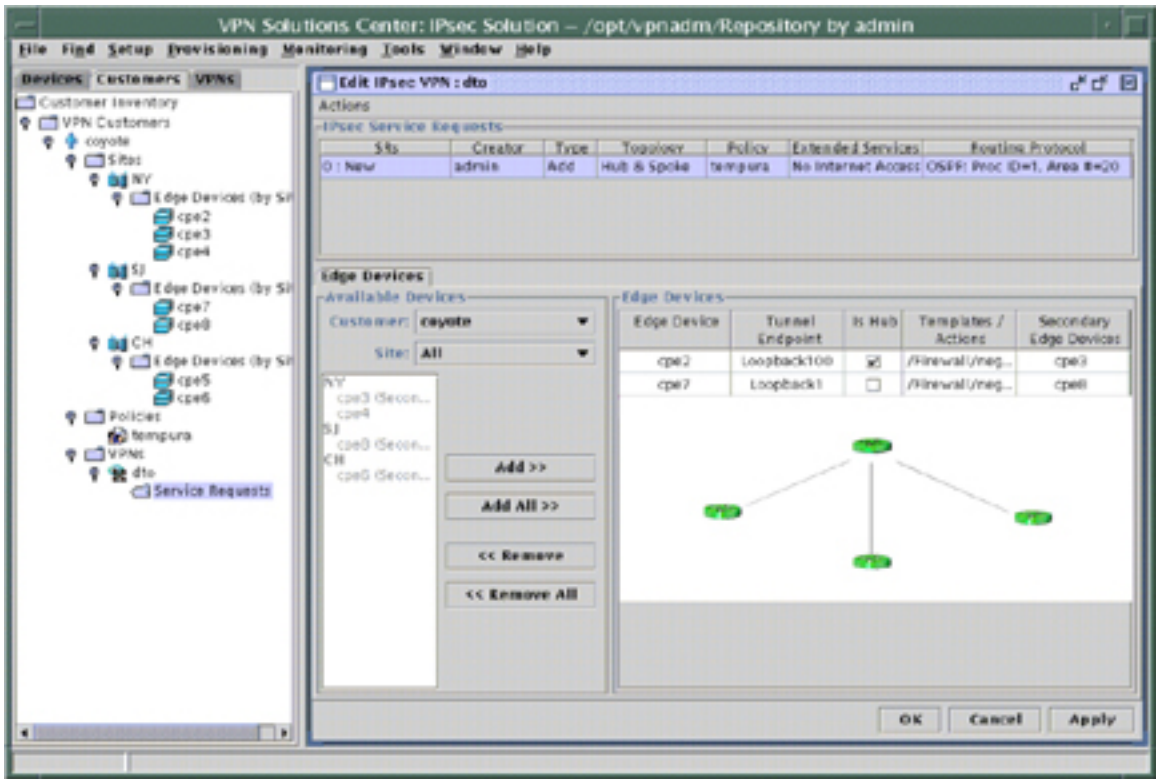
Cisco VPN Solution Center provides management of VPN services throughout the service life cycle including service provisioning and activation on routers, service auditing, and SLAs. The set of well-defined CORBA APIs provide external OSSs access to the full capability of Cisco VPN Solution Center, allowing flow-through provisioning and SLA monitoring.

The Cisco VPN Solution Center complements Cisco VPN solutions by simplifying the planning, provisioning, and service-assurance processes, thereby reducing the cost of deploying and operating VPN services. Operators and upstream systems can add, delete, or modify customer IPSec VPNs and define the associated VPN service topology (hub-and-spoke, full, and extranet) via the Cisco VPN

Solution Center user interface or APIs. Cisco VPN Solution Center then translates the VPN service request information into configurations that implement the VPN service and validates the configuration. Cisco VPN Solution Center keeps track of the current VPN state, including error conditions, of the service request and scheduled tasks.

Cisco VPN Solution Center also supports router console provisioning and templates to allow operators to provision other security-related services such as firewall (for both Cisco IOS and PIX Firewall), Network Address Translation (NAT), or even quality of service (QoS). Figure 2 depicts an IPSec VPN module of Cisco VPN Solution Center.

Figure 2
Cisco VPN Cisco VPN Solution Center 2.2: IPSec Solution

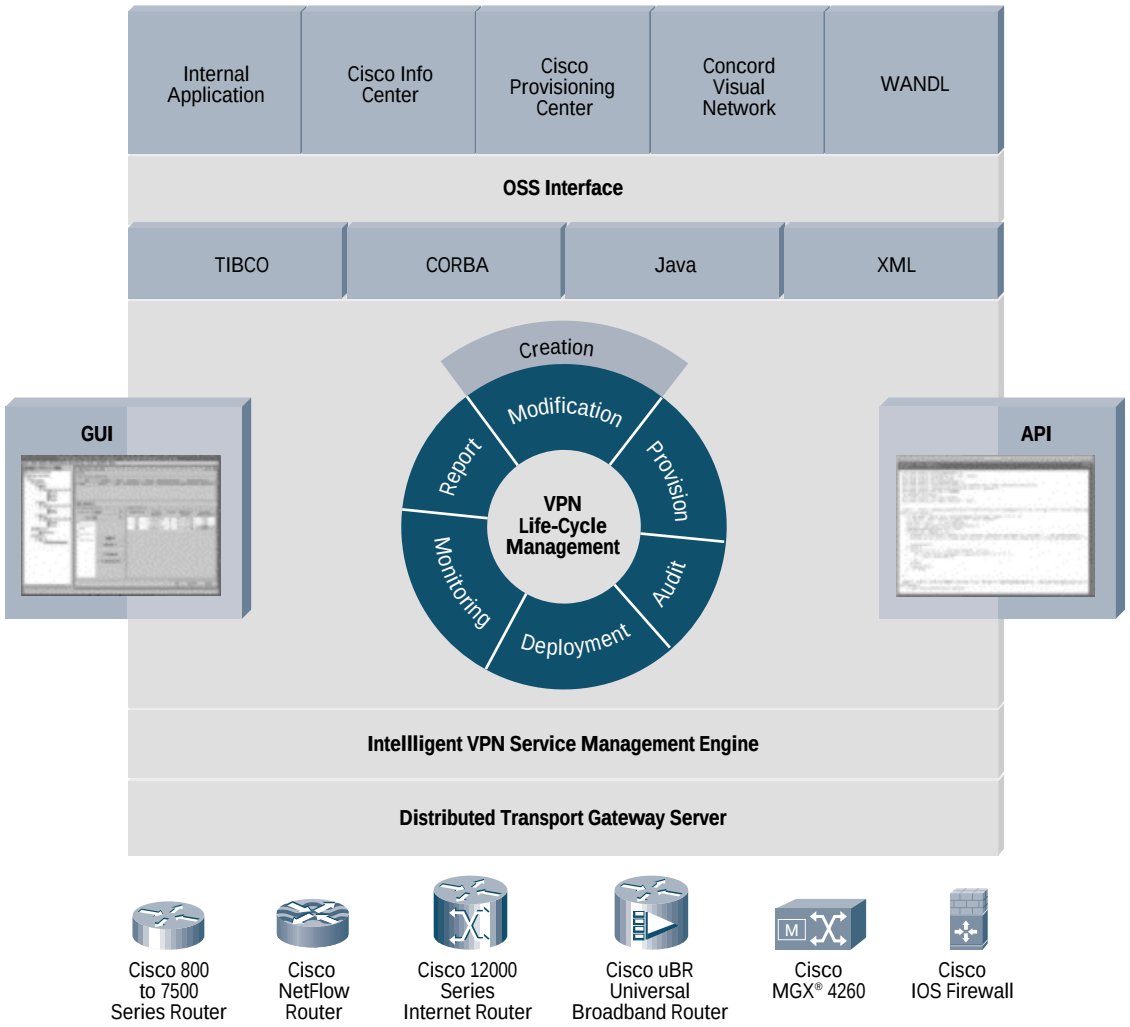


The Cisco VPN Solution Center Approach: Integrated Service-Level Management

The Cisco VPN Solution Center eliminates common deployment and management issues by elevating the service provider's role to that of business manager, as opposed to low-level device-specific policy manager and administrator. The Cisco VPN Solution Center implements a business-centric, service-level-management model that allows the service provider to define high-level policies, while the application of those policies to specific network devices is offloaded to the Cisco VPN Solution Center software (Figure 3).

The Cisco VPN Solution Center IPSec module provides full support for the provisioning and management of LAN-to-LAN VPN services using Cisco IOS customer premises equipment (CPE), Cisco VPN 3000 Series concentrators, and Cisco PIX devices, as well as remote-access VPN services using Cisco VPN 3000 Series concentrators. The Cisco VPN Solution Center MPLS module provides full support for virtually all Cisco provider- and customer-edge devices available.

Figure 3
Cisco VPN Solution Center Architecture API and Life-Cycle Management



Cisco VPN Solution Center Solution: Full VPN Life-Cycle Management

The Cisco VPN Solution Center offers full life-cycle management, from creating the VPN to real-time provisioning, service activation, service auditing, and service assurance. The Cisco VPN Solution Center effectively accommodates the dynamic nature of VPNs, facilitating fast device additions, upgrades, or relocations, and other changes that allow service providers to address the needs of corporate clients. Designed for reliability, scalability, and flexibility, Cisco VPN Solution Center uniquely enables service providers to maintain VPN services with no service disruptions.

Cisco VPN Solution Center Solution Highlights

The Cisco VPN Solution Center provides the provisioning tools that enable rapid deployment and fast time to market of VPN services. The solution also simplifies management of complex, multiaccess, multiplatform VPN services, helping to reduce the service provider's overall administration and management costs. The Cisco VPN Solution Center also features open APIs and OSS interfaces to enable integration of IP VPN services into existing service provider OSSs.

The first layer includes the OSS fault, configuration, and performance applications pre-integrated with the Cisco VPN Solution Center.

- Fault—Cisco Info Center
- Configuration—Cisco Provisioning Center

  - Performance—Concord Network Health Monitor
- The second layer highlights Cisco VPN Solution Center key OSS interfaces, TIBCO event bus for synchronization, (CORBA API) access, and Java and Extensible Markup Language (XML) formatted input/output.
- The third layer focuses on the Cisco VPN Solution Center VPN life-cycle management—The VPN creation can be done via a graphical user interface (GUI), API, or both.
  - The generation of the delta configuration with the intelligent service-management engine enables continuous VPN services; see data sheet for additional information
- A patent-pending, intelligent, service-management engine is the key to automatic generation of the required Cisco IOS Software commands to create the VPN for any protocol (MPLS or IPSec) for any devices, DSL, cable, and all Cisco devices.
- The distributed transport gateway server provides distributed and scalable architecture to communicate with thousands of devices.
- Key to Cisco VPN Solution Center life-cycle management is that Cisco maintains the VPN service during updates with the intelligent Cisco VPN Solution Center Service Management Engine.

Key features of Cisco VPN Solution Center include:

Real-time provisioning—An intelligent provisioning module (the patented Cisco Intelligent Network Engine) captures the intent of the VPN service and translates that intent into an intelligent object model. Based on simple service-order-entry information, the module configures the device and generates the complex instruction sets required to create the VPN. During provisioning requests, the Cisco VPN Solution Center collects real-time configuration and object model information to ensure accuracy.

Automating the complexities of provisioning eliminates many operator errors, shortens service startup times, and lowers the cost of provisioning. The Cisco VPN Solution Center allows customers to create VPN service requests through either GUI or API and manages the entire life cycle for each service request, from service creation to service deployment, service audit, service monitoring, and the service report. Before a VPN is physically deployed, the Cisco VPN Solution Center calculates the delta and generates "configlets" that contain only minimum "necessary" commands that the VPN-involved routers need to know to deliver such a VPN. The same thing happens to modify a VPN.

- *Flexible service activation*—A task scheduler enables operators to schedule the exact date and time of day for service activation. Cisco IOS Software commands the appropriate network elements to activate and then test services.
- *High-performance service auditing*—A high-performance auditor validates IP VPN service configuration, monitors performance, and identifies faults to ensure high network integrity and service quality. The Cisco VPN Solution Center can also generate reports on the status of service requests (requested, pending, deployed, or functional).
- *Service quality assuranc*e—Service-assurance features ensure that VPN target devices remain provisioned correctly and that the VPN itself is operational. Reports and alarms can be generated based on designated requirements, such as SLA thresholds.
- *SLA monitoring and reporting*—A SLA subsystem monitors VPN-aware SLAs for round-trip times, availability, and usage. Thresholds can be configured that allow violations to be reported.
- *QoS provisioning and measurement for service differentiation*—QoS provisioning enables service providers to offer and monitor different classes of service. Using a template engine, the Cisco VPN Solution Center generates router configurations that allocate bandwidth to different classes of service and then measures SLA compliance.
- *Templates for streamlined provisioning*—Cisco VPN Solution Center templates, accessible via the Cisco VPN Solution Center OSS interface or administrative console, allow smart, flexible provisioning of Cisco IOS Software commands. Templates streamline common provisioning functions, making it faster and easier for operators to:
  - Add, delete, and modify Cisco routers above and beyond IP VPN provisioning
  - Establish extranet relationships
  - Provision QoS, core devices, NAT, Hot Standby Router Protocol (HSRP), Cisco IOS firewalls, and Cisco IOS Software command-line interface (CLI) commands
  - Assure high levels of provisioning accuracy via a power scripting language with syntax checking

Application Integration and Flow-Through Provisioning

The Cisco VPN Solution Center operates as a standalone application for the creation of VPNs, or it can be integrated within the larger business application environment for increased efficiencies. The Cisco VPN Solution Center, for example, enhances Cisco Service Management applications such as Cisco Provisioning Center and Cisco Info Center, making them VPN aware and extending Cisco VPN Solution Center capabilities to multivendor environments. The following features extend the functionality of Cisco VPN Solution Center to meet business application requirements and to streamline integration into real-world environments.

- *OSS interface*—CORBA APIs, a TIBCO event bus, and Java and XML interfaces support OSS application integration and flow-through provisioning.
- *Fault management*—The Cisco VPN Solution Center integrates with the Cisco Info Center to provide service-level fault-management functions. Element- and network-level alarms and events can be correlated with service-level information to generate VPN-aware messages.
- *Performance and other extended management functionality*—The Cisco VPN Solution Center can be easily integrated with third-party applications to provide service-level performance management and other extended security and management functions. These applications, provided by Cisco OSS and business support system (BSS) partners through the Cisco Service Provider Solutions Ecosystem, offer service providers a wide range of complementary functionality. Example includes Concord's Network Health Monitor for VPN performance reporting, and Portal and Belle System for IP VPN usage-based billing.

Business Benefits of Cisco VPN Solution Center

The benefits of using Cisco VPN Solution Center for deploying and managing VPN services range from faster time to market to improved network quality, reduced operational costs, and a lower total cost of ownership (TCO). The comprehensive management functionality of the Cisco VPN Solution Center also enables service providers to minimize initial investments by taking full advantage of existing infrastructures and devices.

Cisco VPN Solution Center provides flexibility as well, allowing service providers to implement the most suitable framework—IPSec for traffic that requires robust authentication and confidentiality, and MPLS for broader connectivity and low costs.

In terms of scalability, Cisco VPN Solution Center ensures that service providers can meet both current and future service requirements without having to do a complete equipment upgrade.

New Features in Cisco VPN Solution Center 2.2

Cisco VPN Solution Center Release 2.2 offers new functionality, including:

IPSec-related features:

- Cisco PIX VPN provisioning
- Cisco Easy VPN template
- Cisco IE 2100 integration for "plug and play" VPN deployment

MPLS-related features:

- New ease-of-use provisioning GUI
- Cisco IE 2100 integration for plug-and-play VPN deployment

For More Information

The following Web site offers more information about the Cisco VPN Solution Center: http://www.cisco.com/warp/public/cc/pd/nemnsw/ipvpn/

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

MH/CI/0502