

IP Solution Center—Management for Scalable Security Deployments

With the phenomenal growth of E-commerce, Internet security has become an important and integral component of business, playing a critical role in corporate survival and maintaining competitive advantage.

As enterprises and service providers increasingly deploy security devices throughout their networks, deployment of all those devices and the process of individual device security configuration, such as VPN or Firewall, can cause an exponential increase in operational costs. Individual device security configuration can also lead to inconsistent policies across the network, opening potential security holes. An effective Internet security solution, therefore, is not only about security devices and security technology; it must incorporate the solid management of security technologies.

Introduction

Cisco® IP Solution Center Security technology solution provides enterprises and service providers with a robust and centralized management platform that minimizes operational costs of security and prevents inconsistent security policies. It also enables effective deployment and management throughout the entire lifecycle of security technologies including policy-based VPN, Firewall, NAT and QoS provisioning, policy audit, and integrated security monitoring to security vulnerability reporting (Cisco IP Solution Center is integrated with best-of-breed partner products to provide the security event monitoring and vulnerability reporting features). Cisco ISC has also been tightly integrated with Cisco CNS technology for zero-touch, plug-and-play security CPE deployment.

Cisco IP Solution Center Security Policy Manager allows customers to define global technology-level policies. The software automatically generates device-level

commands and provisions hundreds of thousands of devices accordingly through its powerful internal parallel computation engines. Once the global policies are defined, they can be reused across multiple networks.

A high-performance auditor validates security technology configuration, monitors service accuracy, and identifies faults to ensure high network integrity and service quality. Cisco IP Solution Center can also generate audit reports of service requests, providing a high-performance troubleshooting tool.

As the business and network grow, a huge amount of security devices can be added to the network. Cisco IP Solution Center, working in collaboration with intelligent, embedded Cisco CNS Agent, is able to detect and manage newly added security devices dynamically and automatically. This gives customers the ability to rapidly and dynamically deploy security technologies in a cost-effective manner. Once a new device has been added to the



network, the intelligent, embedded Cisco CNS Agent will inform the Cisco IP Solution Center IE2100 server in real time of all the latest information about that particular device. Subscribing to the CNS Message Bus, Cisco IP Solution Center will then be able to dynamically manage the security policy accordingly. Due to the dynamic nature of a network, device configuration or status can be changed in any time. The intelligent embedded Cisco CNS Agent is capable of informing the Cisco IP Solution Center IE2100 server of all the changes inside security devices, such as change of the DHCP assigned IP address or loopback interface, providing a zero-touch security management environment.

Overview

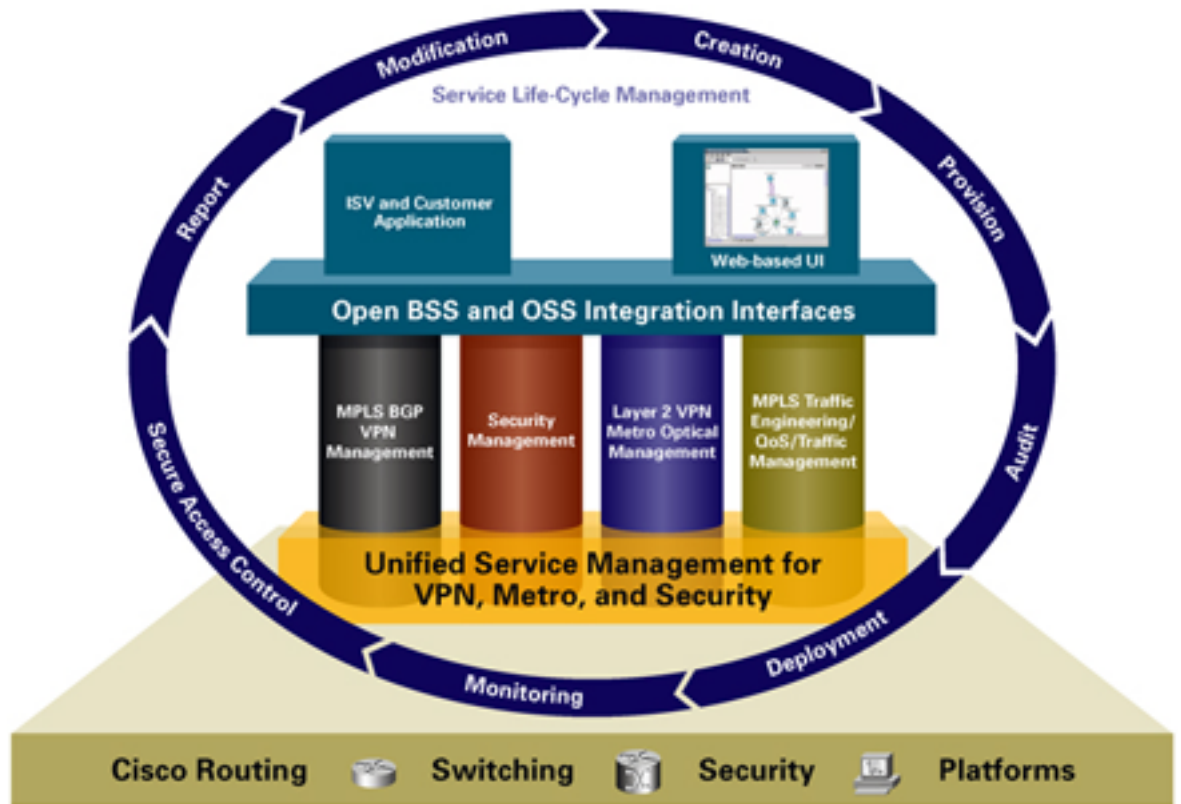
The Cisco IP Solution Center Security management solution eliminates common deployment and management issues by elevating the technology administrator's role to that of business manager, as opposed to low-level, device-specific policy manager and administrator. Cisco IP Solution Center implements a business-centric, policy-level management model that allows customers to define high-level policies, while the application of those policies to specific network devices is offloaded to the ISC software. The Cisco IP Solution Security Management module provides full support for the provisioning and management of LAN-to-LAN VPN, Remote Access VPN, EZ VPN, and DMVPN technologies using Cisco IOS[®] CPEs, VPN 3000 concentrators, and PIX devices, as well as Firewall, NAT, and QoS technologies.

Cisco IP Solution Center provides the software management tools that enable rapid and accurate deployment of security technologies. Simultaneously, the solution simplifies management of complex, multiaccess, multiplatform security technologies, helping to reduce overall administration and management costs. Cisco IP Solution Center also features open application programming interfaces (APIs) such as CORBA, TIBCO, and XML to enable integration of IP security technologies into existing customer operation environments.

Cisco IP Solution Center offers full lifecycle management, from creating the security policy to real-time provisioning, service activation, service auditing, service assurance, and policy reconfiguration. Cisco IP Solution Center was designed to effectively accommodate the dynamic nature of security technologies, facilitating fast additions of devices, device upgrades or relocations, and other changes that allow customers to responsively address the needs of corporate clients. Designed for reliability, scalability, and flexibility, Cisco IP Solution Center uniquely enables customers to maintain security technologies with absolutely no service disruptions.



Figure 1
Cisco IP Solution Center Accurately and Cost-Effectively Manages the Complete Life Cycle of a MPLS VPN Deployment



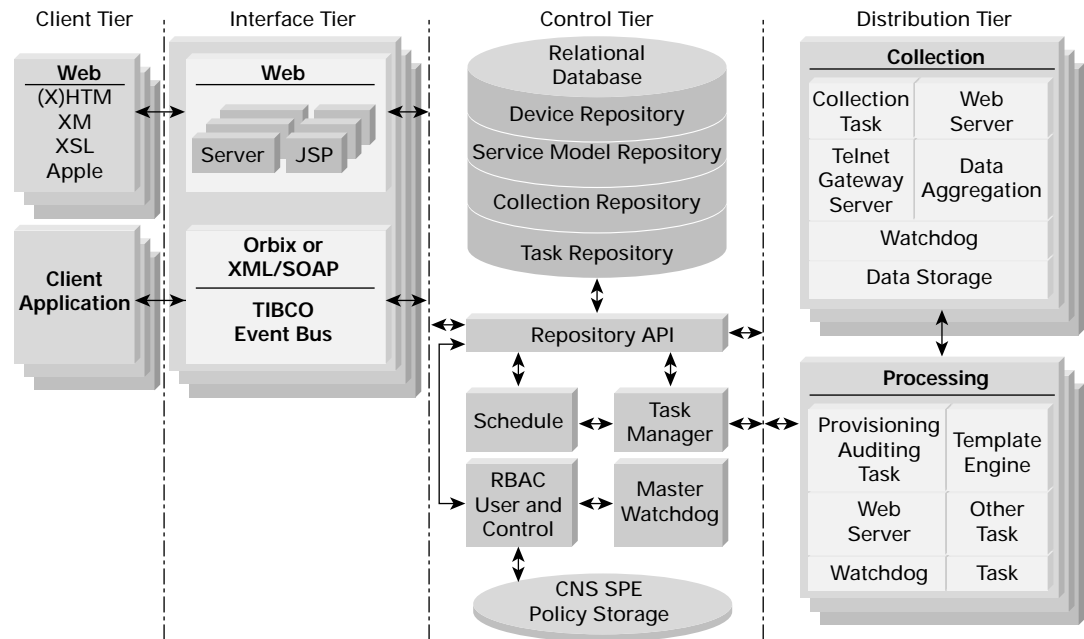
Cisco IP Solution Center System Architecture

Cisco IP Solutions Center is a distributed, four-tier architecture for maximizing scalability, redundancy, and robustness. The four-tier architecture enables the system to scale to large-scale installations as well as standalone, appliance-based installations. The four tiers are: Client, Interface, Control, and Distribution. This architecture provides the modular framework that is the foundation of this scalable, carrier-class system:

- *Client Tier*—Web-based GUI (HTTP to Web server) or client application (RMI to EJB container)
- *Interface Tier*—Scalable J2EE AppServers (Web server and EJB container)
- *Control Tier*—Repository, task manager, watchdog, and scheduler
- *Distribution Tier*—Task worker and collection domain servers



Figure 2
IP Solution Center Architecture



IP Solution Center Security Management Key Features

Easily manage LAN-to-LAN VPN technologies	<ul style="list-style-type: none"> • IPsec tunnel mode • GRE + IPsec transport mode • MGRE + NHRP + IPsec transport mode
Easily manage full-mesh, hub-and-spoke, or partial-mesh VPN topologies	<ul style="list-style-type: none"> • Mass deployment of full-mesh tunnels • Hierarchical hub-and-spoke tunnel provisioning • Partial meshed-tunnel provisioning
Efficiently deploy site-to-site, network-based VPN	<ul style="list-style-type: none"> • IPsec-to-MPLS service mapping • Remote-access VPN, DMVPN, and EZVPN technologies
Manage integrated GRE routing	<ul style="list-style-type: none"> • OSPF • EIGRP • RIP
Design and deploy complex Firewall rules	<ul style="list-style-type: none"> • Support for both Filter Rules and Inspect Rules • Support for URL Filtering Inheritance in device containment hierarchy
Automate fail-over and load balancing configuration	<ul style="list-style-type: none"> • Automatic fail-over back-up VPN provisioning • Automatic load balancing backup hub site provisioning

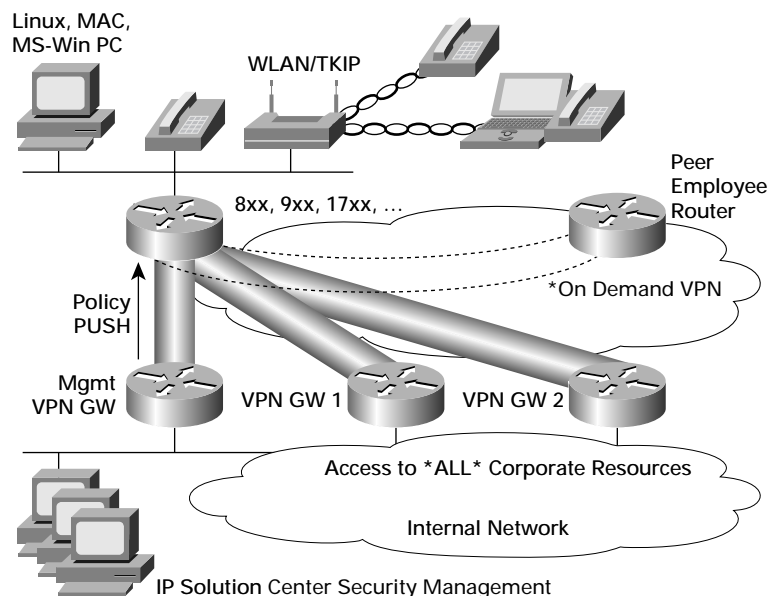


Enable massive NAT configuration deployment	<ul style="list-style-type: none"> • Support for static translation including network-, host-, or port-based translation • Support for dynamic translation including Standard or PAT translation • Support for overlapping address space
Provision Cisco IOS Intrusion Detection System (IDS)	<ul style="list-style-type: none"> • Signature provision and parameter tuning through IDS template
Public Key Infrastructure (PKI) certificate enrollment management	<ul style="list-style-type: none"> • Verify presence of the root cert and device cert for a given trust point's cert chain • Verify re-enrollment of certs according to the auto-enroll percentage parameter • Summary report indicating cert enrollment status or expiration status on desired VPN routers
Flexible template-based sub-provisioning server	<ul style="list-style-type: none"> • User-definable Template Provisioning System for flexible service activation

Leveraging IP Solution Center Security Management for a Large Security Deployment—Case Study

Cisco's Information Technology Department has stringent network security requirements and a need to manage the total cost of ownership (TCO) of deploying security services in a dynamic networking environment, just like many of its customers. And like many of its customers, Cisco has deployed the Cisco IP Solution Center Security Technology Module for zero-touch, plug-and-play security services. Cisco IP Solution Center enables Cisco IT to quickly and cost-effectively deliver secured VPN services, such as dial-up VPN, always-on VPN, and on-demand VPN (DMVPN), to Cisco teleworkers.

Figure 3
Cisco IP Solution Center Deployment at Cisco





Cisco IP Solution Center Security Management provides an environment and a set of tools for provisioning, auditing, and SLA monitoring VPNs. VPN service information, such as the topology (hub-and-spoke or full mesh), IPsec policy, IKE policy, and a list of CPE comprising the VPN, are entered at the VPNSC management console. This information forms a “Service Request” that can then be scheduled to be deployed and audited. The VPN service described in the service request may be augmented with additional IP technologies such as Firewall rules, NAT mappings, QoS policies, and so on.

While deploying a service, Cisco IP Solution Center attempts to upload the current configuration file of each CPE. It then generates a “configlet” containing only commands necessary to enable the VPN, such as the crypto maps, transform sets, IKE policies, crypto ACLs, and so on. Additional commands are also included in the configlet, such as Firewall rules (ACLs and inspect rules), NAT maps, and QoS commands. VPNSC then downloads the IOS CLI Configlets generated for various CPEs in the VPN.

Upon completion of the download, the VPN service is operational. The user may then schedule a task to audit the VPN service on a regular basis. Auditing is the task of uploading the current configuration file of the CPE and ensuring that it contains all necessary service commands. If some commands are missing, an audit report is generated indicating the missing commands. At this point the user can re-deploy the service request to correct the problem. The status of the VPN service is reflected in the state of the service request, which may be Requested, Pending, Deployed, Failed Audit, or Lost.

Cisco IP Solution Center supports a number of transport mechanisms for communicating with the CPE such as SSH, Telnet, TFTP, and CNS. In environments where the IP address of the CPE is dynamically assigned, CNS is the only communication option since SSH and Telnet will not work. In this case study, CNS is used. A Cisco IP Solution Center IE2100 server leverages the CNS event bus to communicate with the routers (for example, to send CLI commands or obtain the full configuration file of a router).

Figure 4
Cisco IP Solution Center Topology View





The goal is to completely automate the process of provisioning the spokes of the Cisco intranet VPN, which uses a hub-and-spoke topology in which the spokes are SOHO routers such as Cisco 806, 827, 905, 1710, and 1750. Auto provisioning of SOHO routers in this case study involves two steps:

Pre-provisioning step: Pre-provisioning the router with a minimum set of commands

Actual provisioning step: Full provisioning of IPsec and other services such as NAT, Firewall, QoS, and DHCP server on the routers

The purpose of pre-provisioning is to equip the SOHO routers with a minimum set of commands so that they can be shipped to user's homes where the final stage of provisioning can be completed. This implies that basic IPv4 connectivity will be provided during this stage. The commands downloaded to the SOHO router during this pre-provisioning stage fall into two groups:

The first group involves all commands that do not require network connectivity. The commands are:

- hostname
- username and password
- enable secret
- domain name
- IPv4 connectivity: configuration of the ISP-facing interface
- CNS commands: in order for router to contact its Cisco IP Solution Center IE2100 Server
- static routes: needed for cert enrollment
- NTP servers

The second group of commands requires network connectivity. The commands are:

- root cert import
- cert enrollment

Cisco IP Solution Center provides the Template System Tool for pre-provisioning the router. All commands that make up the router's minimum pre-provisioning configuration are placed in a template that contains a series of variables. These variables will have different values for different routers.

The template is then instantiated using a data file for a given SOHO router, which is downloaded via console port to the router. At this point, the SOHO router can be disconnected from the terminal server and shipped to an end-user's home.

Once the device has been received and plugged in, the intelligent Cisco CNS Agent embedded within the device will inform the Cisco IP Solution Center IE2100 server in real time of all the latest information about that particular device. Subscribing to the CNS Message Bus, Cisco IP Solution Center will then be able to dynamically manage the security policy. A management VPN can also be set up at this stage. The Cisco CNS Agent can inform the Cisco IP Solution Center IE2100 server of all the latest information within a security device, such as change of the DHCP assigned IP address or loopback interface, providing a zero-touch security management environment.

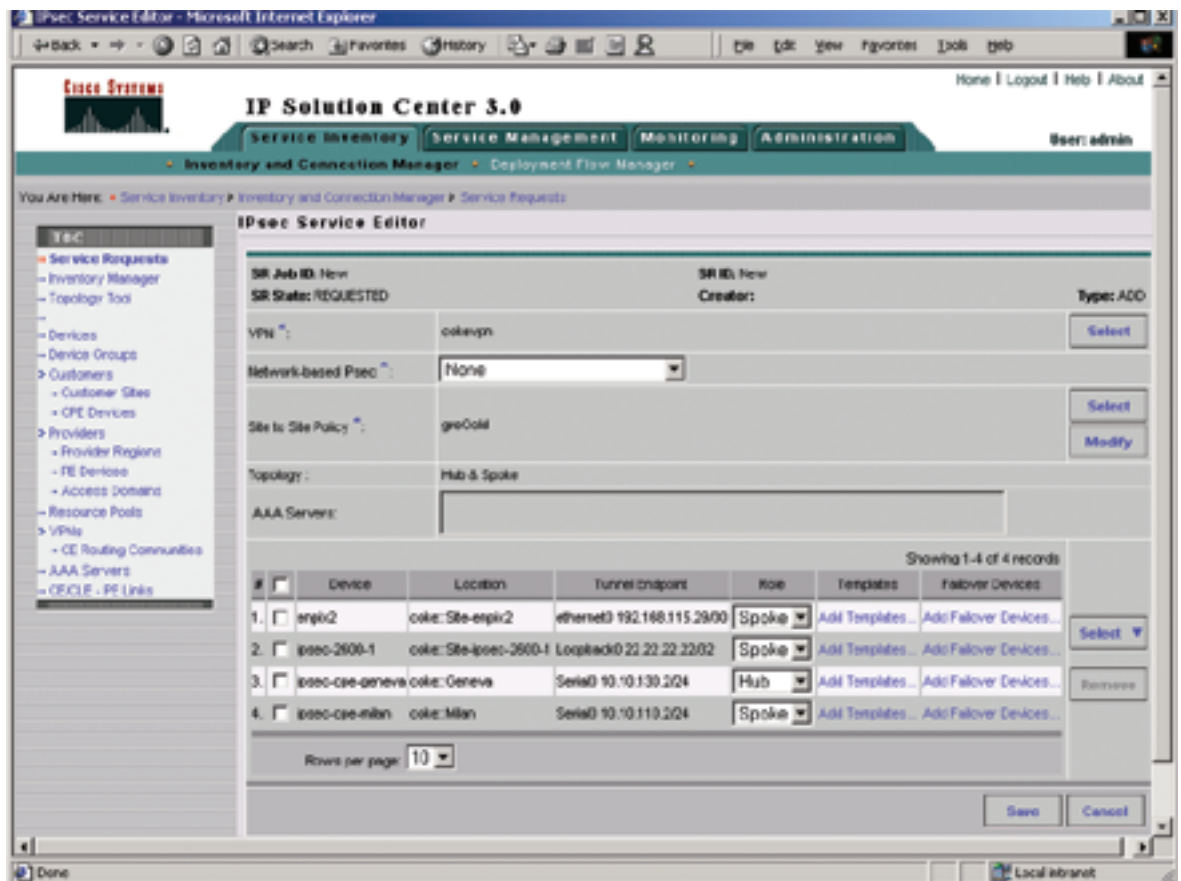
The purpose of full provisioning is to provision the IPsec service on each router, as well as all other necessary services such as Firewall, NAT, QoS, and DHCP server. This step takes place as soon as the pre-provisioned SOHO router has been received and powered on at the end-user's home.



Cisco IP Solution Center supports dynamic IP addresses by using CNS as the transport mechanism for the router. Because it is the router that initiates a connection to the Cisco CNS IE2100 server, its dynamically assigned IP address need not be known by ISC for configuration download. ISC also supports configuration staging on the Cisco CNS IE2100 server by using a CNS pull mechanism. The configuration is stored on the CNS IE2100 server. Whenever the router is powered on, after receiving its connect event, Cisco IP Solution Center will send a trigger to the router asking it to fetch its configuration from the Cisco CNS IE2100 server.

Cisco IP Solution Center provides a centralized service management console and IPsec VPN Service Request Editor to create or modify a VPN service. Once the service request (SR) is created, it is deployed (for example, service IOS CLI Configlets are generated for all routers in the VPN, and they are downloaded to each router). Service modification such as adding or removing routers from a VPN is very simple: just move the router into the selected SR in the VPN editor, or remove the router from the SR, and then save and re-deploy the SR.

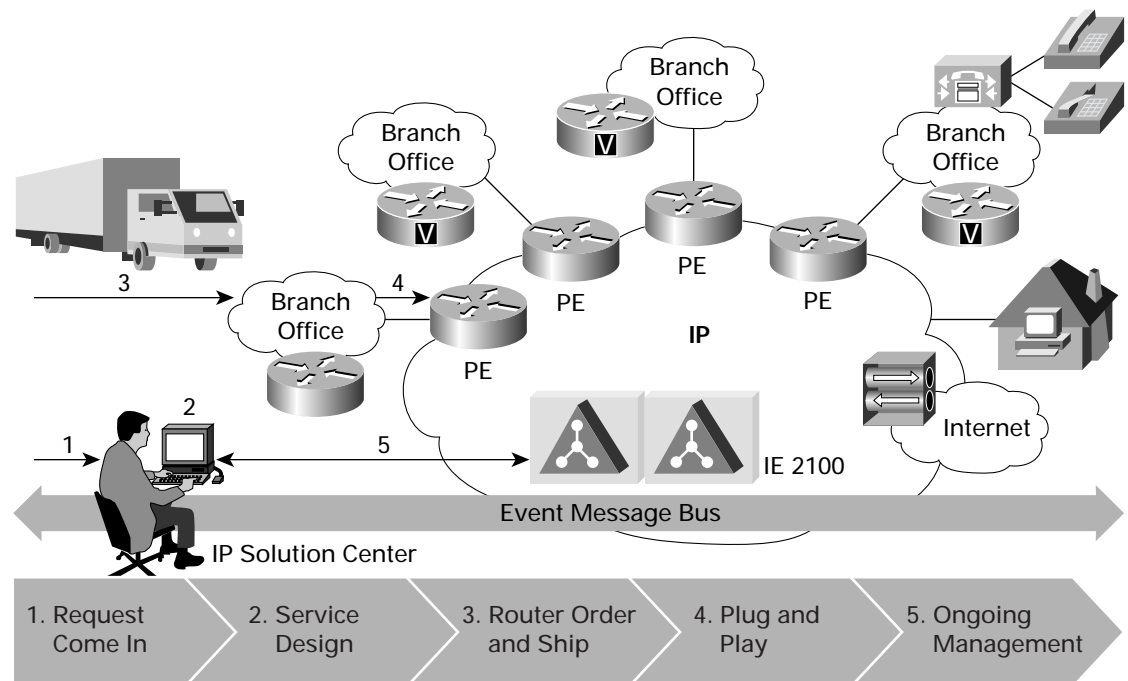
Figure 5
The VPN Service Request Editor is Used to Create or Modify a VPN Service





Cisco IP Solution Center centralized security management platform minimizes Cisco IT security operational costs, prevents inconsistent security policies, and effectively deploys and manages the entire cycle of security service offerings from service request, service design, and service deployment to day-to-day service auditing and monitoring. Cisco IP Solution Center's unique integrated management of policy-based VPN, Firewall, NAT and QoS provisioning, periodic auditing, and security monitoring enables Cisco IT to cost-effectively and accurately deploy large-scale service offerings in a timely manner. It also enables IT to create a solid IP management framework for future service expansion. The following chart illustrates this integrated, end-to-end service-management process:

Figure 6
ISC Provides an Integrated, End-to-End Service-Management Process



Conclusion

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

Cisco IP Solution Center simplifies management of complex multiaccess, multiplatform IP services and reduces management costs. Cisco IP Solution Center service options provide service-level provisioning, service-aware performance and service-level assurance, and service-aware usage. Accepted worldwide by over 160 leading corporations, Cisco IP Solution Center (evolution of well-established Cisco VPNSC) is the standalone management solution for effective management of converging services, supporting a unified view of VPN, Metro Ethernet, security, and QoS services through a common repository of information across all these packet-based services.

Cisco IP Solution Center simplifies and speeds the deployment and management of packet-based services for faster time to revenue while increasing operating efficiencies. It is an end-to-end network management solution that scales as an organization evolves.

Cisco IP Solution Center provides the software management application that enables rapid and accurate deployment of security services. Simultaneously, the solution simplifies management of complex, multiaccess, multiplatform security services. The Cisco IP Solution Center Security Management module provides full support

for the provisioning and management of LAN-to-LAN VPN, Remote Access VPN, EZ VPN, and DMVPN services using Cisco IOS CPEs, VPN 3000 concentrators and PIX devices, as well as Firewall, NAT, and QoS services.

For More Information

Visit the [Cisco IP Solution Center](#) product page for more information.



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, Cisco IOS, Cisco Systems, and the Cisco Systems logo 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) CC/LW4442 0403