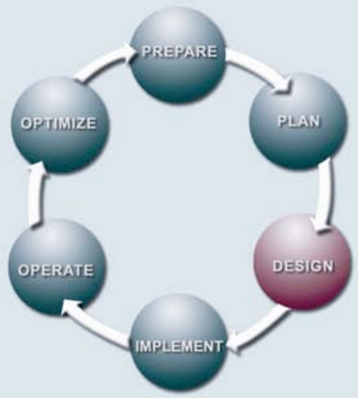
Cisco Security Design Services

Building Integrated Security Solutions to Increase Security, Availability, and Performance

THE CISCO LIFECYCLE SERVICES APPROACH



The unique Cisco Lifecycle approach to services defines the requisite activities at each phase of the network lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled network of partners, and our customers, we achieve the best results.

Network Lifecycle Phases

- **Prepare**—Develop a business case for a technology investment
- **Plan**—Assess readiness to support proposed solution
- **Design**—Create a detailed design to address business and technical requirements
- **Implement**—Deploy new technology
- **Operate**—Maintain network health through day-to-day operations
- **Optimize**—Achieve operational excellence through ongoing improvements

SERVICE OVERVIEW

As the number and complexity of network security threats continues to grow, protecting your corporate network has never been more important. But even when your organization understands the threats that must be addressed, adapting the network security architecture to address them can be difficult. A flawed design can reduce the effectiveness of new security solutions, delay deployment, and increase integration costs.

The Cisco Security Design Services, designed for large enterprises, are a part of the design phase of the Cisco® Lifecycle Services approach. Cisco Systems® consultants can work with your organization to develop a strong security design. The Cisco design methodology considers all aspects of your network security and its integration with your core network infrastructure. Using an in-depth, architectural approach based on industry standards, Cisco security experts can help develop a multilayer defense against directed attacks from hackers or indiscriminate attacks from viruses and worms.

By taking an architectural approach, the security infrastructure designed by Cisco is built to last and can evolve over time to support the deployment of new business applications. Also, by specifying a common set of security solutions, policies, and practices that can be replicated across your organization, Cisco can help reduce your network operating costs by saving time and money on network security administration, lowering your network's total cost of ownership.

The Cisco Security Design services encompass the following two components:

- **Security Design Review** – Review your existing network security design to identify architecture, design, and implementation vulnerabilities and provide recommendations for building, improving, or reengineering your network security design
- **Security Design Development** – Help develop a strategy, plan, and detailed design for integrating enhanced or new security solutions into your network infrastructure

SECURITY DESIGN REVIEW

Aligning the Network Security Design with Business and Security Goals

Cisco network security experts conduct a collaborative review of your organization's business strategy and related security goals, requirements, and standards. Cisco engineers then provide an in-depth analysis of your network security design to determine its effectiveness for meeting your business and IT strategies. Based on analysis of the network information gathered, Cisco engineers provide a detailed review of your network vulnerabilities (Table 1), helping to ensure that the security design meets with proven industry network security design best practices.

After evaluating the existing design for vulnerabilities, Cisco engineers identify and prioritize security requirements for network solutions including intrusion detection, admission control, remote access, endpoint protection, threat mitigation, perimeter control, and VPNs. Cisco can recommend improvements to your network design including network topology, device placement, and connectivity. Taking into consideration all the aspects of your network security – including scalability, performance, and manageability, Cisco can recommend protocol, policy, and feature improvements for individual security components.

Table 1. Security Design Review Activities, Methodology and Deliverable

Activities	Methodology and Deliverable
● Review your network security business goals, objectives, and requirements ● Review your existing network security architecture and design ● Identify and analyze architecture and design vulnerabilities ● Provide a detailed analysis of network security components, including: – Perimeter devices – Network admission control devices – Threat mitigation appliances – Remote-access devices – Intrusion detection systems – Firewalls – Endpoint protection – Routers and switches – Extranet connections – Security management systems ● Recommend improvements to topology, components, functions, and features ● Develop sample configurations for firewalls, NAC devices, threat mitigation devices, intrusion detection systems, endpoint protection, routers, switches, VPNs, access-control servers, wireless devices, and security management tools ● Specify hardware and software requirements including network security management tools ● Provide recommendations for the ongoing management and maintenance of the security solution	**Methodology** ● Conduct a design workshop to gather data and initiate the design review ● Analyze the existing network security design against organizational strategy and requirements ● Provide a preliminary and final gap analysis based on industry best practices ● Deliver an impact analysis of new security requirements on the network infrastructure ● Recommend improvements to the security infrastructure design **Deliverable** ● A Security Design Review document that identifies existing network vulnerabilities; recommends improvements to the overall security design, components, and functions; and provides network diagrams and sample configurations

SECURITY DESIGN DEVELOPMENT

Applying Sound Strategy and Design to the Deployment of New Security Solutions

Security Design Development can help your organization develop a strategy, plan, and design for integrating a new security solution into your core network infrastructure. With this service, Cisco experts can help your organization develop a customized network security design that provides multilayer defense against security threats, shortens implementation times, and smoothes migration associated with deploying a new security solution.

Your organization can avoid potentially costly mistakes or delays by drawing on Cisco expertise across a broad set of network security technologies including network admission control, threat mitigation appliances, intrusion detection, firewalls, remote access, and VPNs (Table 2). By helping prevent costly redesigns to support a new security solution, the service reduces your total cost of ownership of your network and allows your organization to better prepare for future integration and deployment initiatives.

With this service, Cisco consultants and architects conduct a review of your organization's security goals and provide an in-depth analysis of the technical, procedural, and resource requirements for a customized security deployment. After gaining an understanding of your business' security solution goals and requirements, Cisco security experts help develop a design for the security solution including detailed network diagrams and sample configurations that allow for integration into your network environment.

Table 2. Cisco Security Design Development Activities, Methodology, and Deliverable

Activities	Methodology and Deliverable
● Analyze your network security solution goals, objectives, and requirements ● Develop a strategy, plan, and design for a corporate-wide approach to network security ● Evaluate the existing network architecture to identify architecture, design, and implementation vulnerabilities ● Analyze the impact of integrating the new solution with existing IT infrastructure, software operations, and security management procedures ● Assess the network's readiness to deploy the solution, including the current IT infrastructure, security devices, software operations, and security management procedures ● Define the architectural, topological, and functional requirements for the solution ● Develop a detailed design including sample configurations for network security components, including: – Network admission control devices – Threat mitigation appliances – Perimeter devices – Remote-access devices – Intrusion detection systems – Endpoint protection – Firewalls – Routers and switches – Extranet connections – Security management systems ● Specify hardware and software requirements including network security management tools ● Optimize the solution design for scalability, redundancy, and performance ● Provide recommendations for the ongoing management and maintenance of the security solution	**Methodology** ● Conduct a design workshop to gather data and initiate the development of the security design ● Analyze your existing network security architecture against your organizational strategy and requirements ● Develop network security strategy and design specification that meet customized IT and security requirements **Deliverable** ● A Security Design Specification that outlines the overall strategy and plan for the new solution, and defines the security design topology, components, and functions including network diagrams and sample configurations

BENEFITS

With Cisco Security Design services, your organization can:

- Develop a customized network security design that provides a multilayer defense against security threats
- Mitigate network security threats by identifying security vulnerabilities and deviations from corporate security policy and industry best practices
- Improve the reliability, maintainability, and performance of your network security design
- Shorten your implementation and migration times for new security solutions and technologies
- Enhance productivity of your network security staff by reducing the time spent on expensive, time-consuming network redesign
- Mitigate costly delays and problems during design, implementation, and deployment of new security solutions

WHY CISCO

Effective network security begins with a sound network design – a design that incorporates the overarching goals and strategy of your business, as well as the technical security requirements. As part of the Cisco Lifecycle Services approach, Cisco Security Design services allow your organization to better protect business assets and services, more cost-effectively deploy new security solutions, and avoid costly delays and disruptions during integration.

AVAILABILITY AND ORDERING

Cisco Security Design services are available through Cisco and Cisco partners globally. Details may vary by region.

FOR MORE INFORMATION

For more information about the Cisco Security Design services or the Cisco Lifecycle Services approach, contact your Cisco representative.

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

Printed in the USA C78-336450-00 02/06