SDSI - DESIGNING CISCO SECURITY INFRASTRUCTURE V1.0

Course Code: 860044

The Designing Cisco Security Infrastructure (SDSI) training teaches you about security architecture design, including secure infrastructure, applications, risk, events, requirements, artificial intelligence (AI), automation, and DevSecOps.

This training prepares you for the 300-745 SDSI v1.0 exam. If passed, you earn the Cisco Certified Specialist – Designing Cisco Security Infrastructure certification and satisfy the concentration exam requirement for the Cisco Certified Network Professional (CCNP) Security certification.

This training also earns you 41 Continuing Education (CE) credits toward recertification.

What You'll Learn

After completing this course, you should be able to:

- Identify and explain the fundamental concepts of security architecture and how they support the design, building, and maintenance of a secure infrastructure
- Identify the layers of security infrastructure, core security technologies, and infrastructure concepts
- Explain how security designs principles contribute to secure infrastructure
- Identify and discuss security design and management frameworks that can be used for infrastructure security design
- Explain the importance of and methods for enforcement of regulatory compliance in security design
- Identify tools that enable detection and response to infrastructure security incidents
- Explain various strategies that can be implemented to modify traditional security architectures to meet the technical requirements of modern enterprise networks
- Implement secure network access methods, such as 802.1X, MAC Authentication Bypass (MAB), and web-based authentication
- Describe security technologies that can be applied to enterprise Wide Area Network (WAN) connections
- Compare methods to secure network management and control plane traffic

- Compare the differences between traditional firewalls and next-gen firewalls (NGFWs) and identify the advanced features that NGFWs provide
- Explain how web application firewalls (WAFs) secure web applications from threats
- Describe the key features and best practices for deploying intrusion detection system (IDS) and intrusion prevention system (IPS) as part of the enterprise infrastructure security design
- Explain how endpoints and services in cloud-native or microservice environments can be protected with host-based or distributed firewalls
- Discuss security technologies that address application data and data that is in transit
- Identify several security solutions for cloud-native applications, microservices, and containers
- Explain how technology advancements allow for improvements in today's infrastructure security
- Identify tools that enable detection and response to infrastructure security incidents
- Describe frameworks and controls to access and mitigate security risks for infrastructure
- Explain how to make security adjustments following a security incident
- Identify DevSecOps integrations that improve security management and response
- Discuss how to ensure that automated services are secure
- Discuss how AI can aid in threat detection and response

Who Needs to Attend

- Cisco and Partner's Systems Engineers
- Customer Network & Infrastructure Engineers
- Customer Security/NOC Engineers

Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- Cisco CCNP Security or equivalent knowledge
- Familiarity with Microsoft Windows Operating Systems
- Familiarity with the Cisco Security portfolio

These skills can be found in the following Offerings:

SDSI - DESIGNING CISCO SECURITY INFRASTRUCTURE V1.0

Course Code: 860044

VIRTUAL CLASSROOM LIVE	$5,795 CAD	5 Day

Virtual Classroom Live Outline

- Definition and Purpose of Security Architecture
- Components of Security Infrastructure
- Security Design Principles
- Security and Design Frameworks
- Compliance and Regulatory Requirements
- Security Approaches to Protect Against Threats
- Modify the Security Architecture to Meet Technical Requirements
- Network Access Security
- VPN and Tunneling Solutions
- Secure Infrastructure Management and Control Planes
- Nextgen Firewalls
- Web Application Firewall (WAF)
- IPS/IDS Deployment
- Host-Based Firewalls and Distributed Firewalls
- Security Solutions Based on Application and Flow Data
- Security for Cloud-Native Applications, Microservices, and Containers
- Emerging Technologies in Application Security
- SOC Tools for Incident Handling and Response
- Modify Design to Mitigate Risk
- Incident-Driven Security Adjustments
- DevSecOps Integration
- Secure Automated Workflows and Pipelines
- AI’s Role in Securing Infrastructure

Virtual Classroom Live Labs

There are no labs associated with this training.

Oct 13 - 17, 2025 | 9:00 AM - 5:00 PM EDT

Mar 23 - 27, 2026 | 9:00 AM - 5:00 PM EDT

SDSI - DESIGNING CISCO SECURITY INFRASTRUCTURE V1.0

Course Code: 860044

ON-DEMAND	$1,200 CAD

On-Demand Outline

Skills You'll Learn

- Identify and explain fundamental security architecture concepts and how they guide the secure design, building, and maintenance of infrastructure
- Analyze and apply security layers, core technologies, and infrastructure concepts to build robust defenses
- Implement and enforce security design principles, frameworks, and regulatory compliance to align with business and legal requirements
- Deploy and manage detection, response, and access control tools to secure networks, endpoints, and cloud environments
- Adapt and optimize security strategies and architectures to address evolving threats, modern enterprise needs, and technology advancements

Learning Objectives

1. Security Architecture Design Fundamentals: Gain the expertise to design, implement, and sustain comprehensive, compliant, and resilient network security architectures that protect modern enterprise environments and ensure regulatory adherence.
2. Security Architecture for Infrastructure Protection: Develop your abilities to design, implement, and manage comprehensive cybersecurity strategies that enable you to anticipate, mitigate, and respond to threats while ensuring resilient and high-performance digital infrastructure.
3. Firewall Technologies and Advanced Security Solutions: Strengthen your skills to deploy and manage Next-Generation Firewalls, Intrusion Detection and Prevention Systems, and web application security measures to proactively detect, prevent, and respond to advanced cyber threats while ensuring comprehensive protection for your network, endpoints, and web applications.

4. Application Security and Secure Data Flow: Empower yourself to defend your digital assets by mastering strategies for securing web and mobile applications, APIs, and cloud-native environments while gaining insights into how emerging technologies like AI and quantum computing are transforming the application security landscape.
5. Risk Management and Incident Response Strategies: Learn to use SIEM and SOAR tools for real-time incident detection and response, proactively manage risks, and apply industry-standard post-incident recovery strategies to strengthen your organization's security and resilience.
6. DevSecOps Integration and Automated Security Pipelines: Enhance your skills in DevSecOps to ensure security is integral to your CI/CD pipeline, automate secure development workflows, and improve your organization's threat detection and response capabilities.

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 8/30/2025 7:40:55 PM