Designing Cisco Security Infrastructure (SDSI)

Category: Networking & Security | **Vendor:** Cisco

Duration: 40.00 hours (5 days) **32.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Cisco Certified Specialist – Designing Cisco Security Infrastructure, Cisco Certified Network Professional (CCNP) Security, Cisco Certified Specialist - Designing Cisco Security Infrastructure
Related Exam:	300-745

Course Overview

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.

How You'll Benefit

This training will help you:

- Gain hands-on experience of security architecture design
- Qualify for professional and expert-level security job roles
- Prepare for the 300-745 SDSI v1.0 exam
- Earn 41 CE credits toward recertification

What to Expect in the Exam

Designing Cisco Security Infrastructure (300-745 SDSI) v1.0 is a 90-minute exam associated with the Cisco Certified Specialist - Designing Cisco Security Infrastructure certification and satisfies the core exam requirement for the CCNP Security certification.

This exam tests your knowledge of security architecture design, including:

- Secure infrastructure
- Applications
- Risk
- Events
- Requirements

- Artificial intelligence and Automation
- DevSecOps

About This Course

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.

How You'll Benefit

This training will help you:

- Gain hands-on experience of security architecture design
- Qualify for professional and expert-level security job roles
- Prepare for the 300-745 SDSI v1.0 exam
- Earn 41 CE credits toward recertification

What to Expect in the Exam

Designing Cisco Security Infrastructure (300-745 SDSI) v1.0 is a 90-minute exam associated with the Cisco Certified Specialist - Designing Cisco Security Infrastructure certification and satisfies the core exam requirement for the CCNP Security certification.

This exam tests your knowledge of security architecture design, including:

- Secure infrastructure
- Applications
- Risk
- Events
- Requirements

- Artificial intelligence and Automation
- DevSecOps

Who Should Attend

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

Prerequisites & Entry Requirements

General 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 Cisco Learning Offerings:

- Implementing and Operating Cisco Security Core Technologies (SCOR)
- Fundamentals of Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPF)
- Implementing and Configuring Cisco Identity Services Engine (SISE)
- Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)
- Advanced Techniques for Cisco Firewall Threat Defense and Intrusion Prevention (SFWIPA)
- Implementing Secure Solutions with Virtual Private Networks (SVPN)
- Introducing Automation for Cisco Solutions (CSAU)
- Securing Email with Cisco Email Security Appliance (SESA)
- Securing the Web with Cisco Web Security Appliance (SWSA)

Learning Outcomes

Upon successful completion of this course, participants will 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

Detailed Course 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

□□ Certification Path

Cisco Certified Specialist – Designing Cisco Security Infrastructure, Cisco Certified Network Professional (CCNP) Security, Cisco Certified Specialist - Designing Cisco Security Infrastructure

Exam: 300-745

Skills You Will Learn:

- 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

Frequently Asked Questions

Q: What delivery options are available for Designing Cisco Security Infrastructure (SDSI)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The Designing Cisco Security Infrastructure (SDSI) course helps prepare you for the Cisco Certified Specialist – Designing Cisco Security Infrastructure, Cisco Certified Network Professional (CCNP) Security, Cisco Certified Specialist - Designing Cisco Security Infrastructure certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the 300-745 official exam. You can take this exam at any exam center across United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online wherever you are located.

Q: How many CPD hours does this course provide?

The 5-day Designing Cisco Security Infrastructure (SDSI) course provides up to 32.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Designing Cisco Security Infrastructure (SDSI) training?

The training takes place over 5 day(s), with each day lasting approximately 40.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Designing Cisco Security Infrastructure (SDSI)?

Yes, we provide corporate training, dedicated training, and closed classes for Designing Cisco Security Infrastructure (SDSI). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Designing Cisco Security Infrastructure, Cisco Professional Level Security - CCNP, SDSI

Q: Why choose Nexus Human for Designing Cisco Security Infrastructure (SDSI)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Designing Cisco Security Infrastructure (SDSI) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 889 8700 (Ireland) | +44 20 8142 8961 (UK)

© 2026 Nexus Human. All rights reserved. This brochure was generated on 14/11/2026.