Implementing and Operating Cisco Security Core Technologies (SCOR)

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 - Security Core, Cisco Certified Internetwork Expert (CCIE) Security certifications, CCNP
Related Exam:	350-701

Course Overview

The Implementing and Operating Cisco Security Core Technologies (SCOR) training helps you gain the skills and technologies needed to implement core Cisco security solutions. This training will ready you to provide advanced threat protection against cybersecurity attacks and prepare you for senior-level security roles.

This training prepares you for the 350-701 SCOR v1.1 exam. If passed, you earn the Cisco Certified Specialist - Security Core certification and satisfy the core exam requirement for the Cisco Certified Network Professional (CCNP) Security and Cisco Certified Internetwork Expert (CCIE) Security certifications. This training also earns you 64 Continuing Education (CE) credits towards recertification.

Please note that this course lab access is extended for 1 week following the ILT session, for students to complete all additional self-study lab exercises.

How You'll Benefit

This training will help you:

- Gain hands-on experience implementing core security technologies and learn best practices using Cisco security solutions
- Qualify for professional and expert-level security job roles
- Prepare for the 350-701 SCOR v1.1 exam
- Earn 64 CE credits towards recertification

What to Expect in the Exam

Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) v1.1 is a 120-minute exam associated with the Cisco Certified Specialist - Security Core certification and satisfies the core exam requirement for the CCNP Security and CCIE Security certifications.

This exam tests your knowledge of implementing and operating core security technologies, including:

- Network security
- Cloud security
- Content security
- Endpoint protection and detection
- Secure network access
- Visibility and enforcement

Exclusive to Fast Lane / iTLS:

Extended lab hours after the course

About This Course

The Implementing and Operating Cisco Security Core Technologies (SCOR) training helps you gain the skills and technologies needed to implement core Cisco security solutions. This training will ready you to provide advanced threat protection against cybersecurity attacks and prepare you for senior-level security roles.

This training prepares you for the 350-701 SCOR v1.1 exam. If passed, you earn the Cisco Certified Specialist - Security Core certification and satisfy the core exam requirement for the Cisco Certified Network Professional (CCNP) Security and Cisco Certified Internetwork Expert (CCIE) Security certifications. This training also earns you 64 Continuing Education (CE) credits towards recertification.

Please note that this course lab access is extended for 1 week following the ILT session, for students to complete all additional self-study lab exercises.

How You'll Benefit

This training will help you:

- Gain hands-on experience implementing core security technologies and learn best practices using Cisco security solutions
- Qualify for professional and expert-level security job roles
- Prepare for the 350-701 SCOR v1.1 exam
- Earn 64 CE credits towards recertification

What to Expect in the Exam

Implementing and Operating Cisco Security Core Technologies (350-701 SCOR) v1.1 is a 120-minute exam associated with the Cisco Certified Specialist - Security Core certification and satisfies the core exam requirement for the CCNP Security and CCIE Security certifications.

This exam tests your knowledge of implementing and operating core security technologies, including:

- Network security
- Cloud security
- Content security
- Endpoint protection and detection
- Secure network access
- Visibility and enforcement

Exclusive to Fast Lane / iTLS:

Extended lab hours after the course

Who Should Attend

- Security Engineers
- Network Engineers
- Network Designers
- Network Administrators
- Systems Engineers
- Consulting Systems Engineers
- Technical Solutions Architects
- Cisco Integrators and Partners
- Network Managers
- Program Managers
- Project Managers

Prerequisites & Entry Requirements

General Prerequisites:

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

- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts
- Familiarity with basics of networking security concept

s

These skills can be found in the following Cisco Learning Offering:

- Implementing and Administering Cisco Solutions (CCNA)

Learning Outcomes

Upon successful completion of this course, participants will be able to:

After taking this course, you should be able to:

- Describe information security concepts and strategies within the network
- Describe security flaws in the transmission protocol/internet protocol (TCP/IP) and how they can be used to attack networks and hosts
- Describe network application-based attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on Cisco Secure Firewall Adaptive Security Appliance (ASA)
- Deploy Cisco Secure Firewall Threat Defense basic configurations
- Deploy Cisco Secure Firewall Threat Defense IPS, malware, and fire policies
- Deploy Cisco Secure Email Gateway basic configurations
- Deploy Cisco Secure Email Gateway policy configurations
- Describe and implement basic web content security features and functions provided by Cisco Secure Web Appliance
- Describe various attack techniques against the endpoints
- Describe Cisco Umbrella® security capabilities, deployment models, policy management, and Investigate console
- Provide basic understanding of endpoint security and be familiar with common endpoint security technologies
- Describe Cisco Secure Endpoint architecture and basic features
- Describe Cisco Secure Network Access solutions
- Describe 802.1X and extensible authentication protocol (EAP) authentication
- Configure devices for 802.1X operations
- Introduce VPNs and describe cryptography solutions and algorithms
- Describe Cisco secure site-to-site connectivity solutions
- Deploy Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs
- Configure point-to-point IPsec VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense
- Describe Cisco secure remote access connectivity solutions

- Deploy Cisco secure remote access connectivity solutions
- Provide an overview of network infrastructure protection controls
- Examine various defenses on Cisco devices that protect the control plane
- Configure and verify Cisco IOS software layer 2 data plane controls
- Configure and verify Cisco IOS software and Cisco ASA layer 3 data plane controls
- Examine various defenses on Cisco devices that protect the management plane
- Describe the baseline forms of telemetry recommended for network infrastructure and security devices
- Describe deploying Cisco Secure Network Analytics
- Describe basics of cloud computing and common cloud attacks
- Describe how to secure cloud environment
- Describe the deployment of Cisco Secure Cloud Analytics
- Describe basics of software-defined networks and network programmability

Detailed Course Outline

- Network Security Technologies
- Cisco Secure Firewall ASA Deployment
- Cisco Secure Firewall Threat Defense Basics
- Cisco Secure Firewall Threat Defense IPS, Malware, and File Policies
- Cisco Secure Email Gateway Basics
- Cisco Secure Email Policy Configuration
- Cisco Secure Web Appliance Deployment
- VPN Technologies and Cryptography Concepts
- Cisco Secure Site-to-Site VPN Solutions
- Cisco IOS VTI-Based Point-to-Point IPsec VPNs
- Point-to-Point IPsec VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense
- Cisco Secure Remote-Access VPN Solutions
- Remote-Access SSL VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense
- Describing Information Security Concepts
- Describe Common TCP/IP Attacks
- Describe Common Network Application Attacks
- Common Endpoint Attacks

- Cisco Umbrella Deployment
- Endpoint Security Technologies
- Cisco Secure Endpoint
- Cisco Secure Network Access Solutions
- 802.1X Authentication
- 802.1X Authentication Configuration
- Network Infrastructure Protection
- Control Plane Security Solutions
- Layer 2 Data Plane Security Controls
- Layer 3 Data Plane Security Controls
- Management Plane Security Controls
- Traffic Telemetry Methods
- Cisco Secure Network Analytics Deployment
- Cloud Computing and Cloud Security
- Cloud Security
- Cisco Secure Cloud Analytics Deployment
- Software-Defined Networking

□□ Certification Path

Cisco Certified Specialist - Security Core, Cisco Certified Internetwork Expert (CCIE) Security certifications, CCNP

Exam: 350-701

Skills You Will Learn:

After taking this course, you should be able to:

- Describe information security concepts and strategies within the network
- Describe security flaws in the transmission protocol/internet protocol (TCP/IP) and how they can be used to attack networks and hosts
- Describe network application-based attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on Cisco Secure Firewall Adaptive Security Appliance (ASA)
- Deploy Cisco Secure Firewall Threat Defense basic configurations
- Deploy Cisco Secure Firewall Threat Defense IPS, malware, and fire policies
- Deploy Cisco Secure Email Gateway basic configurations
- Deploy Cisco Secure Email Gateway policy configurations
- Describe and implement basic web content security features and functions provided by Cisco Secure Web Appliance
- Describe various attack techniques against the endpoints
- Describe Cisco Umbrella® security capabilities, deployment models, policy management, and Investigate console
- Provide basic understanding of endpoint security and be familiar with common endpoint security technologies
- Describe Cisco Secure Endpoint architecture and basic features
- Describe Cisco Secure Network Access solutions
- Describe 802.1X and extensible authentication protocol (EAP) authentication
- Configure devices for 802.1X operations
- Introduce VPNs and describe cryptography solutions and algorithms
- Describe Cisco secure site-to-site connectivity solutions
- Deploy Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs
- Configure point-to-point IPsec VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense
- Describe Cisco secure remote access connectivity solutions
- Deploy Cisco secure remote access connectivity solutions
- Provide an overview of network infrastructure protection controls
- Examine various defenses on Cisco devices that protect the control plane
- Configure and verify Cisco IOS software layer 2 data plane controls
- Configure and verify Cisco IOS software and Cisco ASA layer 3 data plane controls
- Examine various defenses on Cisco devices that protect the management plane
- Describe the baseline forms of telemetry recommended for network infrastructure and security devices
- Describe deploying Cisco Secure Network Analytics
- Describe basics of cloud computing and common cloud attacks
- Describe how to secure cloud environment
- Describe the deployment of Cisco Secure Cloud Analytics
- Describe basics of software-defined networks and network programmability

Frequently Asked Questions

Q: What delivery options are available for Implementing and Operating Cisco Security Core Technologies (SCOR)?

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 Implementing and Operating Cisco Security Core Technologies (SCOR) course helps prepare you for the Cisco Certified Specialist - Security Core, Cisco Certified Internetwork Expert (CCIE) Security certifications, CCNP certification path.

Q: Which exam does this course prepare me for?

This course prepares you for the 350-701 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 Implementing and Operating Cisco Security Core Technologies (SCOR) 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 Implementing and Operating Cisco Security Core Technologies (SCOR) 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 Implementing and Operating Cisco Security Core Technologies (SCOR)?

Yes, we provide corporate training, dedicated training, and closed classes for Implementing and Operating Cisco Security Core Technologies (SCOR). 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: Implementing and Operating Cisco Security Core Technologies, Cisco Professional Level Security - CCNP, SCOR

Q: Why choose Nexus Human for Implementing and Operating Cisco Security Core Technologies (SCOR)?

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 Implementing and Operating Cisco Security Core Technologies (SCOR) 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.