training code: SCOR / ENG DL 5d / EN

Implementing and Operating Cisco Security Core Technologies

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 toward recertification.

Learn more how you may recertify as part of CE to keep certification status active.

Cisco Continuing Education Program - CE

Taking part in authorised training allows you to obtain extra points necessary to maintain certification.

SCOR: 64 points CE

Training recipients

Course Messaging, Outline, and Instructor Requirements

Course Description [25 Word]

The Implementing and Operating Cisco Security Core Technologies (SCOR) training helps you gain the skills and technologies needed to implement core Cisco security solutions.

Course Description [50 Word]

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.

Course Description (full version)

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 toward recertification.

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 toward recertification

Who Should Enroll

- 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

Benefits

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 toward recertification

Training program

Course Outline

1. Network Security Technologies
2. Cisco Secure Firewall ASA Deployment
3. Cisco Secure Firewall Threat Defense Basics
4. Cisco Secure Firewall Threat Defense IPS, Malware, and File Policies
5. Cisco Secure Email Gateway Basics
6. Cisco Secure Email Policy Configuration
7. Cisco Secure Web Appliance Deployment
8. VPN Technologies and Cryptography Concepts
9. Cisco Secure Site-to-Site VPN Solutions
10. Cisco IOS VTI-Based Point-to-Point IPsec VPNs
11. Point-to-Point IPsec VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense
12. Cisco Secure Remote-Access VPN Solutions
13. Remote-Access SSL VPNs on the Cisco Secure Firewall ASA and Cisco Secure Firewall Threat Defense
14. Describing Information Security Concepts
15. Describe Common TCP/IP Attacks
16. Describe Common Network Application Attacks
17. Common Endpoint Attacks
18. Cisco Umbrella Deployment
19. Endpoint Security Technologies
20. Cisco Secure Endpoint
21. Cisco Secure Network Access Solutions
22. 802.1X Authentication
23. 802.1X Authentication Configuration
24. Network Infrastructure Protection
25. Control Plane Security Solutions
26. Layer 2 Data Plane Security Controls

27. Layer 3 Data Plane Security Controls
28. Management Plane Security Controls
29. Traffic Telemetry Methods
30. Cisco Secure Network Analytics Deployment
31. Cloud Computing and Cloud Security
32. Cloud Security
33. Cisco Secure Cloud Analytics Deployment
34. Software-Defined Networking

Lab Outline

1. Configure Network Settings and NAT on Cisco Secure Firewall ASA
2. Configure Cisco Secure Firewall ASA Access Control Policies
3. Configure Cisco Secure Firewall Threat Defense NAT
4. Configure Cisco Secure Firewall Threat Defense Access Control Policy
5. Configure Cisco Secure Firewall Threat Defense Discovery and IPS Policy
6. Configure Cisco Secure Firewall Threat Defense Malware and File Policy
7. Configure Listener, HAT, and RAT on Cisco Email Secure Email Gateway
8. Configure Cisco Secure Email Policies
9. Configure Proxy Services, Authentication, and HTTPS Decryption
10. Enforce Acceptable Use Control and Malware Protection
11. Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
12. Configure Point-to-Point VPN between Cisco Secure Firewall Threat Defense Devices
13. Configure Remote Access VPN on the Cisco Secure Firewall Threat Defense
14. Examine Cisco Umbrella Dashboard and DNS Security
15. Examine Cisco Umbrella Secure Web Gateway and Cloud-Delivered Firewall
16. Explore Cisco Umbrella CASB Functionalities
17. Explore Cisco Secure Endpoint
18. Perform Endpoint Analysis Using Cisco Secure Endpoint Console
19. Explore File Ransomware Protection by Cisco Secure Endpoint Console
20. Explore Secure Network Analytics v7.4.2
21. Explore Global Threat Alerts Integration and ETA Cryptographic Audit
22. Explore Cloud Analytics Dashboard and Operations
23. Explore Secure Cloud Private and Public Cloud Monitoring

Expected preparation of the participant

There are no 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 concepts

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

- Implementing and Administering Cisco Solutions (CCNA®)

Training Includes

- 5 days with instructor and hands-on lab practice, plus the equivalent of 3 days of self-paced material
- Trainer’s supervision
- Contact with community
- Coursebook
- Lab environment

Training method

- lecture
- workshops

Language

- Training: English
- Materials: English

Duration

5 days / 35 hours

Examination description

The training prepares you for the **350-701 SCOR**, exam, which can be taken for an additional fee at the **PearsonVUE center**. You can also take the exam on-line.
Details are available at: https://home.pearsonvue.com/cisco/onvue