

350-701: CCNP Security Core (SCOR)

Secure networks, cloud workloads, content and endpoints with Cisco technologies, aligned to the SCOR 350-701 exam.

DURATION

5 days · 40 hours

LEVEL

Advanced

CURRICULUM

15 modules · 5 labs

DELIVERYLive online, Onsite,
Corporate

Course overview

Security engineers today protect far more than a perimeter firewall. They secure remote users, cloud workloads, email and web traffic, endpoints and the network fabric itself, often with tools that share threat intelligence and are managed through APIs. SCOR is the core exam for CCNP Security and covers this full span. This five-day course prepares you for it with practical, scenario-based labs.

Day one establishes security concepts: common threats and attacks in on-premises and cloud environments, cryptography, VPN types and secure software practices. Day two covers network security, including next-generation firewalls and intrusion prevention, segmentation, management options and site-to-site and remote access VPNs. Day three looks at securing the cloud, from shared responsibility and DevSecOps to workload and application protection, and then content security for web and email. Day four focuses on endpoint protection and detection, along with secure network access, visibility and enforcement using 802.1X, MAB, TrustSec concepts and NetFlow. Day five brings everything together with security automation through APIs and finishes with exam preparation.

Labs walk you through configuring firewall policies and IPS, building site-to-site and remote access VPNs, setting up 802.1X authentication, exploring web and email security policies and calling security product APIs with Python.

This course is aligned to the Cisco SCOR 350-701 exam. Cisco can revise exam topics, so confirm the current version and pricing with Cisco before booking.

Highlights

- 40 hours of live, trainer-led sessions
- Covers all six SCOR exam topic areas
- Firewall, VPN, 802.1X and segmentation labs
- Security automation with APIs
- Mock exam with detailed review

What's included

- Trainer with enterprise security engineering experience
- Plan aligned to the six SCOR topic areas
- Firewall, IPS and VPN configuration labs
- 802.1X and network access control exercises
- Security API automation with Python
- Mock exam with review
- Course completion certificate from Ace Skills Consulting

Who this course is for

Who should attend

- Network security engineers
- Network engineers moving into security
- Security operations and architecture professionals
- Engineers preparing for CCNP Security

Prerequisites

- CCNA-level networking knowledge
- Basic understanding of security concepts, ideally at Security+ level
- Familiarity with Cisco IOS

Detailed curriculum — 5 days, 40 hours, 15 modules, 5 hands-on labs

Day 1 Security Concepts

8 hours

1.1 Threats and vulnerabilities

- Common attacks on networks and applications
- Vulnerabilities such as injection and buffer overflow
- Cloud-specific threats

1.2 Cryptography

- Symmetric and asymmetric encryption
- PKI and certificates
- Hashing and digital signatures

1.3 VPN concepts

- IPsec fundamentals
- DMVPN, FlexVPN and SSL VPN overview
- Site-to-site vs remote access

1.4 Security intelligence

- Threat intelligence sharing
- Secure coding concepts
- Security response and logging

Day 2 Network Security

8 hours

2.1 Firewalls and IPS

- Next-generation firewall features
- Deployment modes
- Access control and intrusion policies

LAB Build firewall access and intrusion policies · 55 min

2.2 Segmentation and management

- Segmentation with VLANs and VRFs
- Secure management plane
- Device management options

2.3 VPN implementation

- Site-to-site IPsec configuration
- Troubleshooting VPNs
- Remote access VPN configuration

LAB Configure site-to-site and remote access VPNs · 55 min

Day 3 Cloud and Content Security

8 hours

3.1 Securing the cloud

- Shared responsibility
- Workload and application protection
- DevSecOps concepts
- Cloud logging and monitoring

3.2 Web security

- Web proxy deployment
- DNS-layer security
- URL filtering and malware scanning

LAB Create web and DNS security policies · 40 min

3.3 Email security

- Email threats
- Data loss prevention for email
- Inbound and outbound policies

Day 4 Endpoint Protection and Secure Network Access

8 hours

4.1 Endpoint protection and detection

- EPP vs EDR
- Device posture and MDM
- Outbreak control and quarantine

4.2 Network access control

- 802.1X and MAB
- Guest and BYOD access
- RADIUS and change of authorisation

LAB Configure 802.1X authentication with a RADIUS server · 55 min

4.3 Visibility and enforcement

- NetFlow and telemetry
- Application visibility and control
- Exfiltration detection

Day 5 Security Automation and Exam Readiness

8 hours

5.1 Automation

- REST APIs for security products
- Event-driven responses
- Python scripts for queries and changes

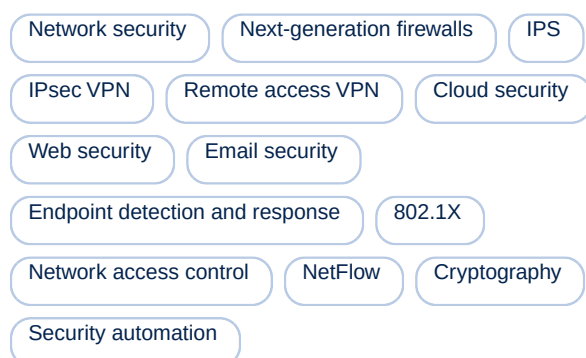
LAB Query and update a security product with Python · 45 min

5.2 Exam readiness

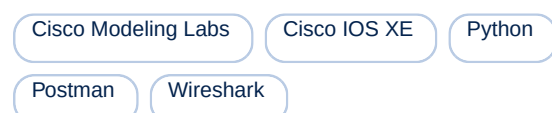
- Domain review
- Study plan
- Mock exam and review

Skills and tools

Skills you will build



Tools used in class



Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam	Implementing and Operating Cisco Security Core Technologies (SCOR)
Exam code	350-701
Duration	120 minutes
Delivery	Online proctored, Test centre
Official page	https://www.cisco.com/site/us/en/learn/training-certifications/certifications/security/ccnp-security/index

Exam skill areas covered

Security Concepts, Security Fundamentals, Security Operations, Security Monitoring and Detection, and Enforcement

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

Does SCOR alone give me CCNP Security?

No. CCNP Security requires SCOR plus one concentration exam. Passing SCOR alone earns a Cisco specialist certification.

Do the labs use real Cisco security products?

Labs combine Cisco emulation for network devices with demonstrations and sandbox environments for cloud-delivered products. Ask for the current lab list before enrolling.

Is the exam fee included?

Only when the batch shows the "Exam voucher included" badge. Otherwise you book directly with Cisco through Pearson VUE.

I am new to security. Is this course right for me?

It suits engineers with solid networking and basic security knowledge. If you are new to security, consider Security+ or the Cisco Cybersecurity Associate course first.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/350-701-ccnp-security-core-scor · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur
New Delhi 110092
Office: 98180 12523

Cisco, CCNA and CCNP are trademarks of Cisco Systems, Inc. All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website. Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.