Implementing and Operating Cisco Security Core Technologies Training

Duration: **5 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

This course provides in-depth technical training on the implementation, operation, and management of core Cisco security technologies. Participants develop practical skills for configuring, managing, and troubleshooting security solutions designed to protect organisations against advanced cyber threats.

The programme supports preparation for the **Cisco 350-701 SCOR v1.0** exam and contributes towards achieving the **Cisco Certified Specialist – Security Core** certification. It also fulfils the core exam requirement for the CCNP Security and CCIE Security certification paths. The course also provides **64 Continuing Education (CE) credits** that may be used towards recertification.

Key areas include network security, cloud security, endpoint protection, secure network access, VPN technologies, cryptography, security visibility, and policy enforcement.

Hands-on labs and realistic scenarios give participants practical experience with Cisco security technologies and help reinforce the operational skills required in real environments.

Prerequisites

There are no formal prerequisites for attending this course.

However, participants will benefit from prior knowledge of:

- Ethernet and TCP/IP networking,
- Windows operating system administration,
- Cisco IOS networking concepts,
- Basic network security principles.

A CCNA-level understanding of networking can provide a useful foundation.

Who Should Attend

This course is particularly suitable for:

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

Implementing and Operating Cisco Security Core Technologies Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this course, participants will be able to:

- Explain key information security concepts and security strategies,
- Identify TCP/IP vulnerabilities and common exploitation methods,
- Describe network application-based attacks and mitigation techniques,
- Configure access control on Cisco Secure Firewall Adaptive Security Appliance (ASA),
- Deploy and manage Cisco Secure Firewall Threat Defense policies,
- Implement Cisco Secure Email Gateway and web security capabilities,
- Explain endpoint security threats and Cisco Umbrella capabilities,
- Configure 802.1X authentication and secure network access,
- Implement VPN and cryptographic technologies,
- Deploy site-to-site and remote-access VPN solutions,
- Describe and configure network infrastructure protection mechanisms,
- Understand cloud security with Cisco Secure Cloud Analytics,
- Explain the role of Software-Defined Networking (SDN) and network programmability in security.

Training Outline

Network Security Technologies

- Core security concepts
- Common network threats
- Cisco Secure Firewall ASA deployment
- ASA basic configuration
- Access Control Policies
- Cisco Secure Firewall Threat Defense
- Threat Defense basic configuration
- Intrusion Prevention
- Malware Protection
- File Policies
- Network security policy enforcement

Content Security Technologies

- Cisco Secure Email Gateway deployment
- Email security configuration
- Policy-based email controls
- Spam, phishing, and malicious content risks
- Cisco Secure Web Appliance
- Web security capabilities
- Web filtering and policy enforcement
- Content security implementation scenarios

Endpoint Protection and Security Visibility

- Common endpoint attacks
- Endpoint threat prevention
- Cisco Secure Endpoint architecture

- Cisco Secure Endpoint capabilities
- Endpoint telemetry
- Cisco Umbrella
- Umbrella deployment models
- Policy management
- DNS-layer security
- Security visibility

Secure Network Access and Enforcement

- Cisco Secure Network Access solutions
- Identity-based network access
- 802.1X Authentication
- Extensible Authentication Protocol (EAP)
- EAP Methods
- Endpoint and network device authentication
- Configuring devices for 802.1X operations
- Access enforcement

VPN Technologies and Cryptographic Solutions

- Introduction to VPN technologies
- Encryption methods
- Cryptographic concepts
- Secure Site-to-Site VPNs
- Cisco IOS Virtual Tunnel Interface (VTI)
- IPsec VPN
- Point-to-Point IPsec VPN
- Configuring IPsec on Cisco Secure Firewall
- Remote Access VPN concepts
- Secure tunnel management

Network Infrastructure Protection

- Control Plane Security
- Layer 2 Data Plane Controls
- Layer 3 Data Plane Controls
- Management Plane Security
- Network infrastructure hardening
- Telemetry
- Network Monitoring
- Monitoring security devices
- Visibility and control across security infrastructure

Cloud Security and SDN

- Cloud Security risks
- Cloud Security best practices
- Cisco Secure Cloud Analytics
- Cloud-based threat visibility
- Deploying Secure Cloud Analytics
- Software-Defined Networking (SDN)

BILGINÇ IT Academy

info@bilginc.com

bilginc.com

- Network Programmability
- The role of SDN in security operations
- Automation and programmable security concepts

Exams and Assessments

This course supports preparation for the **Cisco 350-701 SCOR v1.0** exam.

The exam:

- Has an approximate duration of 120 minutes,
- Covers core Cisco Security Technologies,
- Contributes to the Cisco Certified Specialist – Security Core certification,
- Satisfies the core exam requirement for CCNP Security and CCIE Security.

The exam cost is not included with this course and is available separately.

Hands-On Learning

Participants complete practical exercises throughout the programme.

Hands-on activities include:

- Configuring Cisco security solutions,
- Troubleshooting security configurations,
- Implementing Access Control Policies,
- Deploying VPN solutions,
- Configuring Endpoint Protection,
- Analysing security threats,
- Using Cisco security tools,
- Deploying secure cloud environments,
- Applying network security enforcement scenarios.

This practical approach helps learners apply Cisco security technologies in realistic operational environments.