



Implementing and Operating Cisco Security Core Technologies v1.1 (350-701)

Exam Description: Implementing and Operating Cisco Security Core Technologies v1.1 (SCOR 350-701) is a 120-minute exam associated with the CCNP and CCIE Security Certifications. This exam tests a candidate's knowledge of implementing and operating core security technologies including network security, cloud security, content security, endpoint protection and detection, secure network access, visibility, and enforcements. The course, Implementing and Operating Cisco Security Core Technologies, helps candidates to prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

- 25%** **1.0** **Security Concepts**
 - 1.1 Explain common threats against on-premises, hybrid, and cloud environments
 - 1.1.a On-premises: viruses, trojans, DoS/DDoS attacks, phishing, rootkits, man-in-the-middle attacks, SQL injection, cross-site scripting, malware
 - 1.1.b Cloud: data breaches, insecure APIs, DoS/DDoS, compromised credentials
 - 1.2 Compare common security vulnerabilities such as software bugs, weak and/or hardcoded passwords, OWASP top ten, missing encryption ciphers, buffer overflow, path traversal, cross-site scripting/forgery
 - 1.3 Describe functions of the cryptography components such as hashing, encryption, PKI, SSL, IPsec, NAT-T IPv4 for IPsec, preshared key, and certificate-based authorization
 - 1.4 Compare site-to-site and remote access VPN deployment types and components such as virtual tunnel interfaces, standards-based IPsec, DMVPN, FlexVPN, and Cisco Secure Client including high availability considerations
 - 1.5 Describe security intelligence authoring, sharing, and consumption
 - 1.6 Describe the controls used to protect against phishing and social engineering attacks
 - 1.7 Explain North Bound and South Bound APIs in the SDN architecture
 - 1.8 Explain Cisco DNA Center APIs for network provisioning, optimization, monitoring, and troubleshooting
 - 1.9 Interpret basic Python scripts used to call Cisco Security appliances APIs
- 20%** **2.0** **Network Security**

- 2.1 Compare network security solutions that provide intrusion prevention and firewall capabilities
- 2.2 Describe deployment models of network security solutions and architectures that provide intrusion prevention and firewall capabilities
- 2.3 Describe the components, capabilities, and benefits of NetFlow and Flexible NetFlow records
- 2.4 Configure and verify network infrastructure security methods
 - 2.4.a Layer 2 methods (network segmentation using VLANs; Layer 2 and port security; DHCP snooping; Dynamic ARP inspection; storm control; PVLANS to segregate network traffic; and defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks)
 - 2.4.b Device hardening of network infrastructure security devices (control plane, data plane, and management plane)
- 2.5 Implement segmentation, access control policies, AVC, URL filtering, malware protection, and intrusion policies
- 2.6 Implement management options for network security solutions (single vs. multidevice manager, in-band vs. out-of-band, cloud vs. on-premises)
- 2.7 Configure AAA for device and network access such as TACACS+ and RADIUS
- 2.8 Configure secure network management of perimeter security and infrastructure devices such as SNMPv3, NetConf, RestConf, APIs, secure syslog, and NTP with authentication
- 2.9 Configure and verify site-to-site and remote access VPN
 - 2.9.a Site-to-site VPN using Cisco routers and IOS
 - 2.9.b Remote access VPN using Cisco AnyConnect Secure Mobility client
 - 2.9.c Debug commands to view IPsec tunnel establishment and troubleshooting
- 15%** **3.0 Securing the Cloud**
 - 3.1 Identify security solutions for cloud environments
 - 3.1.a Public, private, hybrid, and community clouds
 - 3.1.b Cloud service models: SaaS, PaaS, IaaS (NIST 800-145)
 - 3.2 Compare security responsibility for the different cloud service models
 - 3.2.a Patch management in the cloud
 - 3.2.b Security assessment in the cloud
 - 3.3 Describe the concept of DevSecOps (CI/CD pipeline, container orchestration, and secure software development)
 - 3.4 Implement application and data security in cloud environments
 - 3.5 Identify security capabilities, deployment models, and policy management to secure the cloud
 - 3.6 Configure cloud logging and monitoring methodologies

- 3.7 Describe application and workload security concepts
- 15% 4.0 Content Security**
 - 4.1 Implement traffic redirection and capture methods for web proxy
 - 4.2 Describe web proxy identity and authentication including transparent user identification
 - 4.3 Compare the components, capabilities, and benefits of on-premises, hybrid, and cloud-based email and web solutions (Cisco Secure Email Gateway, Cisco Secure Email Cloud Gateway, and Cisco Secure Web Appliance)
 - 4.4 Configure and verify web and email security deployment methods to protect on-premises, hybrid, and remote users
 - 4.5 Configure and verify email security features such as SPAM filtering, antimalware filtering, DLP, blocklisting, and email encryption
 - 4.6 Configure and verify Cisco Umbrella Secure Internet Gateway and web security features such as blocklisting, URL filtering, malware scanning, URL categorization, web application filtering, and TLS decryption
 - 4.7 Describe the components, capabilities, and benefits of Cisco Umbrella
 - 4.8 Configure and verify web security controls on Cisco Umbrella (identities, URL content settings, destination lists, and reporting)
- 10% 5.0 Endpoint Protection and Detection**
 - 5.1 Compare Endpoint Protection Platforms (EPP) and Endpoint Detection & Response (EDR) solutions
 - 5.2 Configure endpoint antimalware protection using Cisco Secure Endpoint
 - 5.3 Configure and verify outbreak control and quarantines to limit infection
 - 5.4 Describe justifications for endpoint-based security
 - 5.5 Describe the value of endpoint device management and asset inventory systems such as MDM
 - 5.6 Describe the uses and importance of a multifactor authentication (MFA) strategy
 - 5.7 Describe endpoint posture assessment solutions to ensure endpoint security
 - 5.8 Explain the importance of an endpoint patching strategy
- 15% 6.0 Secure Network Access, Visibility, and Enforcement**
 - 6.1 Describe identity management and secure network access concepts such as guest services, profiling, posture assessment and BYOD
 - 6.2 Configure and verify network access control mechanisms such as 802.1X, MAB, WebAuth
 - 6.3 Describe network access with CoA
 - 6.4 Describe the benefits of device compliance and application control
 - 6.5 Explain exfiltration techniques (DNS tunneling, HTTPS, email, FTP/SSH/SCP/SFTP, ICMP, Messenger, IRC, NTP)
 - 6.6 Describe the benefits of network telemetry
 - 6.7 Describe the components, capabilities, and benefits of these security products and solutions
 - 6.7.a Cisco Secure Network Analytics
 - 6.7.b Cisco Secure Cloud Analytics
 - 6.7.c Cisco pxGrid

- 6.7.d Cisco Umbrella Investigate
- 6.7.e Cisco Cognitive Intelligence
- 6.7.f Cisco Encrypted Traffic Analytics
- 6.7.g Cisco Secure Client Network Visibility Module (NVM)