# CCIE Security Written Exam (350-018) version 4.0

**Exam Description:** The Cisco CCIE® Security Written Exam (350-018) version 4.0 is a 2-hour test with 90–110 questions. This exam tests the skills and competencies of security professionals in terms of describing, implementing, deploying, configuring, maintaining, and troubleshooting Cisco network security solutions and products, as well as current industry best practices and internetworking fundamentals.

Topics include networking fundamentals and security-related concepts and best practices, as well as Cisco network security products and solutions in areas such as VPNs, intrusion prevention, firewalls, identity services, policy management, and device hardening. Content includes both IPv4 and IPv6 concepts and solutions.

The exam is closed book, and no outside reference materials are allowed.

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. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

**20%** **1.0** **Infrastructure, Connectivity, Communications, and Network Security**

- 1.1 Network addressing basics
- 1.2 OSI layers
- 1.3 TCP/UDP/IP protocols
- 1.4 LAN switching (for example, VTP, VLANs, spanning tree, and trunking)
- 1.5 Routing protocols (for example, RIP, EIGRP, OSPF, and BGP)
  - .5.a Basic functions and characteristics
  - 1.5.b Security features
- 1.6 Tunneling protocols
  - 1.6.a GRE
  - 1.6.b NHRP
  - 1.6.c IPv6 tunnel types
- 1.7 IP multicast
  - 1.7.a PIM
  - 1.7.b MSDP
  - 1.7.c IGMP and CGMP
  - 1.7.d Multicast Listener Discovery

1.8 Wireless
- 1.8.a SSID
- 1.8.b Authentication and authorization
- 1.8.c Rogue APs
- 1.8.d Session establishment

1.9 Authentication and authorization technologies
- 1.9.a Single sign-on
- 1.9.b OTPs
- 1.9.c LDAP and AD
- 1.9.d RBAC

1.10 VPNs
- 1.10.a L2 vs L3
- 1.10.b MPLS, VRFs, and tag switching

1.11 Mobile IP networks

**15% 2.0 Security Protocols**

2.1 RSA
2.2 RC4
2.3 MD5
2.4 SHA
2.5 DES
2.6 3DES
2.7 AES
2.8 IPsec
2.9 ISAKMP
2.10 IKE and IKEv2
2.11 GDOI
2.12 AH
2.13 ESP
2.14 CEP
2.15 TLS and DTLS
2.16 SSL
2.17 SSH
2.18 RADIUS
2.19 TACACS+
2.20 LDAP
2.21 EAP methods (for example, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, and LEAP)
2.22 PKI, PKIX, and PKCS
2.23 IEEE 802.1X
2.24 WEP, WPA, and WPA2
2.25 WCCP
2.26 SXP
2.27 MACsec
2.28 DNSSEC

**10% 3.0 Application and Infrastructure Security**

- 3.1 HTTP
- 3.2 HTTPS
- 3.3 SMTP
- 3.4 DHCP
- 3.5 DNS
- 3.6 FTP and SFTP
- 3.7 TFTP
- 3.8 NTP
- 3.9 SNMP
- 3.10 syslog
- 3.11 Netlogon, NetBIOS, and SMB
- 3.12 RPCs
- 3.13 RDP and VNC
- 3.14 PCoIP
- 3.15 OWASP
- 3.16 Manage unnecessary services

**10% 4.0 Threats, Vulnerability Analysis, and Mitigation**

- 4.1 Recognize and mitigate common attacks
  - 4.1.a ICMP attacks and PING floods
  - 4.1.b MITM
  - 4.1.c Replay
  - 4.1.d Spoofing
  - 4.1.e Backdoor
  - 4.1.f Botnets
  - 4.1.g Wireless attacks
  - 4.1.h DoS and DDoS attacks
  - 4.1.i Virus and worm outbreaks
  - 4.1.j Header attacks
  - 4.1.k Tunneling attacks
- 4.2 Software and OS exploits
- 4.3 Security and attack tools
- 4.4 Generic network intrusion prevention concepts
- 4.5 Packet filtering
- 4.6 Content filtering and packet inspection
- 4.7 Endpoint and posture assessment
- 4.8 QoS marking attacks

**20% 5.0 Cisco Security Products, Features, and Management**

5.1 Cisco Adaptive Security Appliance (ASA)
- 5.1.a Firewall functionality
- 5.1.b Routing and multicast capabilities
- 5.1.c Firewall modes
- 5.1.d NAT (before and after version 8.4)
- 5.1.e Object definition and ACLs
- 5.1.f MPF functionality (IPS, QoS, and application awareness)
- 5.1.g Context-aware firewall
- 5.1.h Identity-based services
- 5.1.i Failover options

5.2 Cisco IOS firewalls and NAT
- 5.2.a CBAC
- 5.2.b Zone-based firewall
- 5.2.c Port-to-application mapping
- 5.2.d Identity-based firewalling

5.3 Cisco Intrusion Prevention Systems (IPS)

5.4 Cisco IOS IPS

5.5 Cisco AAA protocols and application
- 5.5.a RADIUS
- 5.5.b TACACS+
- 5.5.c Device administration
- 5.5.d Network access
- 5.5.e IEEE 802.1X
- 5.5.f VSAs

5.6 Cisco Identity Services Engine (ISE)

5.7 Cisco Secure ACS Solution Engine

5.8 Cisco Network Admission Control (NAC) Appliance Server

5.9 Endpoint and client
- 5.9.a Cisco AnyConnect VPN Client
- 5.9.b Cisco VPN Client
- 5.9.c Cisco Secure Desktop
- 5.9.d Cisco NAC Agent

5.10 Secure access gateways (Cisco IOS router or ASA)
- 5.10.a IPsec
- 5.10.b SSL VPN
- 5.10.c PKI

5.11 Virtual security gateway

5.12 Cisco Catalyst 6500 Series ASA Services Modules

5.13 ScanSafe functionality and components

5.14 Cisco Web Security Appliance and Cisco Email Security Appliance

5.15 Security management
- 5.15.a Cisco Security Manager
- 5.15.b Cisco Adaptive Security Device Manager (ASDM)
- 5.15.c Cisco IPS Device Manager (IDM)
- 5.15.d Cisco IPS Manager Express (IME)
- 5.15.e Cisco Configuration Professional
- 5.15.f Cisco Prime

**17% 6.0 Cisco Security Technologies and Solutions**

6.1 Router hardening features (for example, CoPP, MPP, uRPF, and PBR)

6.2 Switch security features (for example, anti-spoofing, port, STP, MACSEC, NDAC, and NEAT)

6.3 NetFlow

6.4 Wireless security

6.5 Network segregation
- 6.5.a VRF-aware technologies
- 6.5.b VXLAN

6.6 VPN solutions
- 6.6.a FlexVPN
- 6.6.b DMVPN
- 6.6.c GET VPN
- 6.6.d Cisco EasyVPN

6.7 Content and packet filtering

6.8 QoS application for security

6.9 Load balancing and failover

**8% 7.0 Security Policies and Procedures, Best Practices, and Standards**

7.1 Security policy elements
7.2 Information security standards (for example, ISO/IEC 27001 and ISO/IEC 27002)
7.3 Standards bodies (for example, ISO, IEC, ITU, ISOC, IETF, IAB, IANA, and ICANN)
7.4 Industry best practices (for example, SOX and PCI DSS)
7.5 Common RFC and BCP (for example, RFC2827/BCP38, RFC3704/BCP84, and RFC5735)
7.6 Security audit and validation
7.7 Risk assessment

7.8 Change management process
7.9 Incident response framework
7.10 Computer security forensics
7.11 Desktop security risk assessment and desktop security risk management