CCIE Security (400-251)

Exam Description: The CCIE Security Version 5.0 exam unifies written and practical exam topics documents into a unique curriculum, while explicitly disclosing which domains pertain to which exam, and the relative weight of each domain.

The Cisco CCIE Security **Written Exam** (400-251) version 5.0 is a two-hour test with 90–110 questions that validate professionals who have the expertise to describe, design, implement, operate, and troubleshoot complex security technologies and solutions. Candidates must understand the requirements of network security, how different components interoperate, and translate it into the device configurations. The exam is closed book and no outside reference materials are allowed.

The Cisco CCIE Security **Lab Exam** version 5.0 is an eight-hour, hands-on exam that requires a candidate to plan, design, implement, operate, and troubleshoot complex security scenarios for a given specification. Knowledge of troubleshooting is an important skill and candidates are expected to diagnose and solve issues as part of the CCIE lab 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. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

Domain Number	Domain	Written Exam Percentage (%)	Lab Exam Percentage (%)
1.0	Perimeter Security and Intrusion Prevention	21	23
2.0	Advanced Threat Protection and Content Security	17	19
3.0	Secure Connectivity and Segmentation	17	19
4.0	Identity Management, Information Exchange, and Access Control	22	24
5.0	Infrastructure Security, Virtualization, and Automation	13	15
6.0	Evolving Technologies	10	N/A
	Total %	100	100

1.0 Perimeter Security and Intrusion Prevention

1.1 Describe, implement, and troubleshoot HA features on Cisco ASA and Cisco FirePOWER Threat Defense (FTD)

1.2 Describe, implement, and troubleshoot clustering on Cisco ASA and Cisco FTD

1.3 Describe, implement, troubleshoot, and secure routing protocols on Cisco ASA and Cisco FTD

1.4 Describe, implement, and troubleshoot different deployment modes such as routed, transparent, single, and multicontext on Cisco ASA and Cisco FTD

1.5 Describe, implement, and troubleshoot firewall features such as NAT (v4,v6), PAT, application inspection, traffic zones, policy-based routing, traffic redirection to service modules, and identity firewall on Cisco ASA and Cisco FTD

1.6 Describe, implement, and troubleshoot IOS security features such as Zone-Based Firewall (ZBF), application layer inspection, NAT (v4,v6), PAT and TCP intercept on Cisco IOS/IOS-XE

1.7 Describe, implement, optimize, and troubleshoot policies and rules for traffic control on Cisco ASA, Cisco FirePOWER and Cisco FTD

1.8 Describe, implement, and troubleshoot Cisco Firepower Management Center (FMC) features such as alerting, logging, and reporting

1.9 Describe, implement, and troubleshoot correlation and remediation rules on Cisco FMC

1.10 Describe, implement, and troubleshoot Cisco FirePOWER and Cisco FTD deployment such as in-line, passive, and TAP modes

1.11 Describe, implement, and troubleshoot Next Generation Firewall (NGFW) features such as SSL inspection, user identity, geolocation, and AVC (Firepower appliance)

1.12 Describe, detect, and mitigate common types of attacks such as DoS/DDoS, evasion techniques, spoofing, man-in-the-middle, and botnet

2.0 Advanced Threat Protection and Content Security

2.1 Compare and contrast different AMP solutions including public and private cloud deployment models

2.2 Describe, implement, and troubleshoot AMP for networks, AMP for endpoints, and AMP for content security (CWS, ESA, and WSA)

2.3 Detect, analyze, and mitigate malware incidents

2.4 Describe the benefit of threat intelligence provided by AMP Threat GRID

2.5 Perform packet capture and analysis using Wireshark, tcpdump, SPAN, and RSPAN

2.6 Describe, implement, and troubleshoot web filtering, user identification, and Application Visibility and Control (AVC)

2.7 Describe, implement, and troubleshoot mail policies, DLP, email quarantines, and SenderBase on ESA

2.8 Describe, implement, and troubleshoot SMTP authentication such as SPF and DKIM on ESA

2.9 Describe, implement, and troubleshoot SMTP encryption on ESA

2.10 Compare and contrast different LDAP query types on ESA

2.11 Describe, implement, and troubleshoot WCCP redirection

2.12 Compare and contrast different proxy methods such as SOCKS, Auto proxy/WPAD, and transparent

2.13 Describe, implement, and troubleshoot HTTPS decryption and DLP

2.14 Describe, implement, and troubleshoot CWS connectors on Cisco IOS routers, Cisco ASA, Cisco AnyConnect, and WSA

2.15 Describe the security benefits of leveraging the OpenDNS solution.

2.16 Describe, implement, and troubleshoot SMA for centralized content security management

2.17 Describe the security benefits of leveraging Lancope

3.0 Secure Connectivity and Segmentation

3.1 Compare and contrast cryptographic and hash algorithms such as AES, DES, 3DES, ECC, SHA, and MD5

3.2 Compare and contrast security protocols such as ISAKMP/IKEv1, IKEv2, SSL, TLS/DTLS, ESP, AH, SAP, and MKA

3.3 Describe, implementc and troubleshoot remote access VPN using technologies such as FLEXVPN, SSL-VPN between Cisco firewalls, routers, and end hosts

3.4 Describe, implement, and troubleshoot the Cisco IOS CA for VPN authentication

3.5 Describe, implement, and troubleshoot clientless SSL VPN technologies with DAP and smart tunnels on Cisco ASA and Cisco FTD

3.6 Describe, implement, and troubleshoot site-to-site VPNs such as GETVPN, DMVPN and IPsec

3.7 Describe, implement, and troubleshoot uplink and downlink MACsec (802.1AE)

3.8 Describe, implement, and troubleshoot VPN high availability using Cisco ASA VPN clustering and dual-hub DMVPN deployments

3.9 Describe the functions and security implications of cryptographic protocols such as AES, DES, 3DES, ECC, SHA, MD5, ISAKMP/IKEv1, IKEv2, SSL, TLS/DTLS, ESP, AH, SAP, MKA, RSA, SCEP/EST, GDOI, X.509, WPA, WPA2, WEP, and TKIP

3.10 Describe the security benefits of network segmentation and isolation

3.11 Describe, implement, and troubleshoot VRF-Lite and VRF-Aware VPN

3.12 Describe, implement, and troubleshoot microsegmentation with TrustSec using SGT and SXP

3.13 Describe, implement, and troubleshoot infrastructure segmentation methods such as VLAN, PVLAN, and GRE

3.14 Describe the functionality of Cisco VSG used to secure virtual environments

3.15 Describe the security benefits of data center segmentation using ACI, EVPN, VXLAN, and NVGRE

4.0 Identity Management, Information Exchange, and Access Control

4.1 Describe, implement, and troubleshoot various personas of ISE in a multinode deployment

4.2 Describe, implement, and troubleshoot network access device (NAD), ISE, and ACS configuration for AAA

4.3 Describe, implement, and troubleshoot AAA for administrative access to Cisco network devices using ISE and ACS

4.4 Describe, implement, verify, and troubleshoot AAA for network access with 802.1X and MAB using ISE.

4.5 Describe, implement, verify, and troubleshoot cut-through proxy/auth-proxy using ISE as the AAA server

4.6 Describe, implement, verify, and troubleshoot guest life cycle management using ISE and Cisco network infrastructure

4.7 Describe, implement, verify, and troubleshoot BYOD on-boarding and network access flows with an internal or external CA

4.8 Describe, implement, verify, and troubleshoot ISE and ACS integration with external identity sources such as LDAP, AD, and external RADIUS

4.9 Describe ISE and ACS integration with external identity sources such as RADIUS Token, RSA SecurID, and SAML

4.10 Describe, implement, verify, and troubleshoot provisioning of AnyConnect with ISE and ASA

4.11 Describe, implement, verify, and troubleshoot posture assessment with ISE

4.12 Describe, implement, verify, and troubleshoot endpoint profiling using ISE and Cisco network infrastructure including device sensor

4.13 Describe, implement, verify, and troubleshoot integration of MDM with ISE

4.14 Describe, implement, verify, and troubleshoot certificate based authentication using ISE

4.15 Describe, implement, verify, and troubleshoot authentication methods such as EAP Chaining and Machine Access Restriction (MAR)

4.16 Describe the functions and security implications of AAA protocols such as RADIUS, TACACS+, LDAP/LDAPS, EAP (EAP-PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-TEAP, EAP-MD5, EAP-GTC), PAP, CHAP, and MS-CHAPv2

4.17 Describe, implement, and troubleshoot identity mapping on ASA, ISE, WSA and FirePOWER

4.18 Describe, implement, and troubleshoot pxGrid between security devices such as WSA, ISE, and Cisco FMC

5.0 Infrastructure Security, Virtualization, and Automation

5.1 Identify common attacks such as Smurf, VLAN hopping, and SYNful knock, and their mitigation techniques

5.2 Describe, implement, and troubleshoot device hardening techniques and control plane protection methods, such as CoPP and IP Source routing.

5.3 Describe, implement, and troubleshoot management plane protection techniques such as CPU and memory thresholding and securing device access

5.4 Describe, implement, and troubleshoot data plane protection techniques such as iACLs, uRPF, QoS, and RTBH

5.5 Describe, implement, and troubleshoot IPv4/v6 routing protocols security

5.6 Describe, implement, and troubleshoot Layer 2 security techniques such as DAI, IPDT, STP security, port security, DHCP snooping, and VACL

5.7 Describe, implement, and troubleshoot wireless security technologies such as WPA, WPA2, TKIP, and AES

5.8 Describe wireless security concepts such as FLEX Connect, wIPS, ANCHOR, Rogue AP, and Management Frame Protection (MFP)

5.9 Describe, implement, and troubleshoot monitoring protocols such as NETFLOW/IPFIX, SNMP, SYSLOG, RMON, NSEL, and eSTREAMER

5.10 Describe the functions and security implications of application protocols such as SSH, TELNET, TFTP, HTTP/HTTPS, SCP, SFTP/FTP, PGP, DNS/DNSSEC, NTP, and DHCP

5.11 Describe the functions and security implications of network protocols such as VTP, 802.1Q, TCP/UDP, CDP, LACP/PAgP, BGP, EIGRP, OSPF/OSPFv3, RIP/RIPng, IGMP/CGMP, PIM, IPv6, and WCCP

5.12 Describe the benefits of virtualizing security functions in the data center using ASAv, WSAv, ESAv, and NGIPSv

5.13 Describe the security principles of ACI such as object models, endpoint groups, policy enforcement, application network profiles, and contracts

5.14 Describe the northbound and southbound APIs of SDN controllers such as APIC-EM

5.15 Identify and implement security features to comply with organizational security policies, procedures, and standards such as BCP 38, ISO 27001, RFC 2827, and PCI-DSS

5.16 Describe and identify key threats to different places in the network (campus, data center, core, edge) as described in Cisco SAFE

5.17 Validate network security design for adherence to Cisco SAFE recommended practices

5.18 Interpret basic scripts that can retrieve and send data using RESTful API calls in scripting languages such as Python

5.19 Describe Cisco Digital Network Architecture (DNA) principles and components.

6.0 Evolving Technologies

6.1 Cloud

6.1.a Compare and contrast cloud deployment models

6.1.a.1 Infrastructure, platform, and software services (XaaS)

6.1.a.2 Performance and reliability

6.1.a.3 Security and privacy

6.1.a.4 Scalability and interoperability

6.1.b Describe cloud implementations and operations

6.1.b.1 Automation and orchestration

6.1.b.2 Workload mobility

6.1.b.3 Troubleshooting and management

6.1.b.4 OpenStack components

6.2 Network Programmability (SDN)

6.2.a Describe functional elements of network programmability (SDN) and how they interact

6.2.a.1 Controllers

6.2.a.2 APIs

6.2.a.3 Scripting

6.2.a.4 Agents

6.2.a.5 Northbound vs. Southbound protocols

6.2.b Describe aspects of virtualization and automation in network environments

6.2.b.1 DevOps methodologies, tools, and workflows

6.2.b.2 Network/application function virtualization (NFV, AFV)

6.2.b.3 Service function chaining

6.2.b.4 Performance, availability, and scaling considerations

6.3 Internet of Things (IoT)

6.3.a Describe architectural framework and deployment considerations for Internet of Things

6.3.a.1 Performance, reliability, and scalability

6.3.a.2 Mobility

6.3.a.3 Security and privacy

6.3.a.4 Standards and compliance

6.3.a.5 Migration

6.3.a.6 Environmental impacts on the network