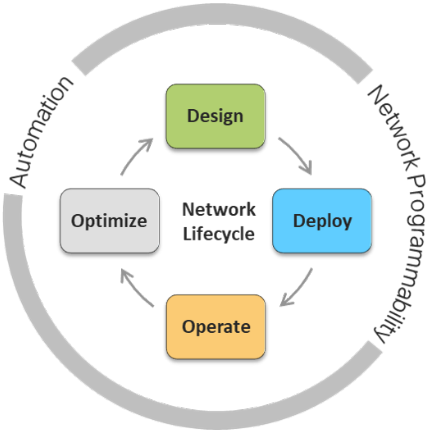
CCIE Security (v6.0) Exam Topics – Practical Exam

Exam Description: The Cisco CCIE Security (v6.0) Practical Exam is an eight-hour, hands-on exam that requires a candidate to plan, design, deploy, operate, and optimize network security solutions to protect your network.



Candidates are expected to program and automate the network within their exam, as per exam topics below.

The following topics are general guidelines for the content likely to be included on the exam. Your knowledge, skills and abilities on these topics will be tested throughout the entire network lifecycle, unless explicitly specified otherwise within this document.

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

1. Perimeter Security and Intrusion Prevention (20%)

1.1 Deployment modes on Cisco ASA and Cisco FTD

- 1.1.a Routed
- 1.1.b Transparent
- 1.1.c Single
- 1.1.d Multi-Context
- 1.1.e Multi-Instance

1.2 Firewall features on Cisco ASA and Cisco FTD

- 1.2.a NAT
- 1.2.b Application inspection
- 1.2.c Traffic zones
- 1.2.d Policy-based routing
- 1.2.e Traffic redirection to service modules
- 1.2.f Identity firewall

1.3 Security features on Cisco IOS/IOS-XE

- 1.3.a Application awareness
- 1.3.b Zone-Based Firewall (ZBFW)
- 1.3.c NAT

1.4 Cisco Firepower Management Center (FMC) features

- 1.4.a Alerting
- 1.4.b Logging
- 1.4.c Reporting

1.5 NGIPS deployment modes

- 1.5.a In-Line
- 1.5.b Passive
- 1.5.c TAP

1.6 Next Generation Firewall (NGFW) features

- 1.6.a SSL inspection
- 1.6.b user identity
- 1.6.c geolocation
- 1.6.d AVC

1.7 Detect, and mitigate common types of attacks

- 1.7.a DoS/DDoS
- 1.7.b Evasion Techniques
- 1.7.c Spoofing
- 1.7.d Man-In-The-Middle
- 1.7.e Botnet

1.8 Clustering/HA features on Cisco ASA and Cisco FTD

1.9 Policies and rules for traffic control on Cisco ASA and Cisco FTD

1.10 Routing protocols security on Cisco IOS, Cisco ASA and Cisco FTD

1.11 Network connectivity through Cisco ASA and Cisco FTD

1.12 Correlation and remediation rules on Cisco FMC

2. Secure Connectivity and Segmentation (20%)

2.1 AnyConnect client-based remote access VPN technologies on Cisco ASA, Cisco FTD, and Cisco Routers.

2.2 Cisco IOS CA for VPN authentication

2.3 FlexVPN, DMVPN, and IPsec L2L Tunnels

2.4 Uplink and downlink MACsec (802.1AE)

2.5 VPN high availability using

- 2.5.a Cisco ASA VPN clustering
- 2.5.b Dual-Hub DMVPN deployments

2.6 Infrastructure segmentation methods

- 2.6.a VLAN
- 2.6.b PVLAN
- 2.6.c GRE
- 2.6.d VRF-Lite

2.7 Micro-segmentation with Cisco TrustSec using SGT and SXP

3. Infrastructure Security (15%)

3.1 Device hardening techniques and control plane protection methods

- 3.1.a CoPP
- 3.1.b IP Source routing
- 3.1.c iACLs

3.2 Management plane protection techniques

- 3.2.a CPU
- 3.2.b Memory thresholding
- 3.2.c Securing device access

3.3 Data plane protection techniques

- 3.3.a uRPF
- 3.3.b QoS
- 3.3.c RTBH

3.4 Layer 2 security techniques

- 3.4.a DAI

3.4.b IPDT
3.4.c STP security
3.4.d Port security
3.4.e DHCP snooping
3.4.f RA Guard
3.4.g VACL

3.5 Wireless security technologies
3.5.a WPA
3.5.b WPA2
3.5.c WPA3
3.5.d TKIP
3.5.e AES

3.6 Monitoring protocols
3.6.a NetFlow/IPFIX/NSEL
3.6.b SNMP
3.6.c SYSLOG
3.6.d RMON
3.6.e eStreamer

3.7 Security features to comply with organizational security policies, procedures, and standards BCP 38
3.7.a ISO 27001
3.7.b RFC 2827
3.7.c PCI-DSS

3.8 Cisco SAFE model to validate network security design and to identify threats to different Places in the Network (PINs)

3.9 Interaction with network devices through APIs using basic Python scripts

3.9.a REST API requests and responses
3.9.a i HTTP action verbs, error codes, cookies, headers
3.9.a ii JSON or XML payload
3.9.a iii Authentication

3.9.b Data encoding formats
3.9.b I JSON
3.9.b ii XML
3.9.b iii YAML

3.10 Cisco DNAC Northbound APIs use cases
3.10.a. Authentication/Authorization

3.10.b. Network Discovery
3.10.c. Network Device
3.10.d. Network Host

4. Identity Management, Information Exchange, and Access Control (25%)

4.1 ISE scalability using multiple nodes and personas.

4.2 Cisco switches and Cisco Wireless LAN Controllers for network access AAA with ISE.

4.3 Cisco devices for administrative access with ISE

4.4 AAA for network access with 802.1X and MAB using ISE.

4.5 Guest lifecycle management using ISE and Cisco Wireless LAN controllers

4.6 BYOD on-boarding and network access flows

4.7 ISE integration with external identity sources
4.7.a LDAP
4.7.b AD
4.7.c External RADIUS

4.8 Provisioning of AnyConnect with ISE and ASA

4.9 Posture assessment with ISE

4.10 Endpoint profiling using ISE and Cisco network infrastructure including device sensor

4.11 Integration of MDM with ISE

4.12 Certificate-based authentication using ISE

4.13 Authentication methods
4.13.a EAP Chaining
4.13.b Machine Access Restriction (MAR)

4.14 Identity mapping on ASA, ISE, WSA, and FTD

4.15 pxGrid integration between security devices WSA, ISE, and Cisco FMC

4.16 Integration of ISE with multi-factor authentication

4.17 Access control and single sign-on using Cisco DUO security technology

5. Advanced Threat Protection and Content Security (20%)

5.1 AMP for networks, AMP for endpoints, and AMP for content security (ESA, and WSA)

5.2 Detect, analyze, and mitigate malware incidents

5.3 Perform packet capture and analysis using Wireshark, tcpdump, SPAN, ERSPAN, and RSPAN

5.4 DNS layer security, intelligent proxy, and user identification using Cisco Umbrella

5.5 Web filtering, user identification, and Application Visibility and Control (AVC) on Cisco FTD and WSA.

5.6 WCCP redirection on Cisco devices

5.7 Email security features
- 5.7.a Mail policies
- 5.7.b DLP
- 5.7.c Quarantine
- 5.7.d Authentication
- 5.7.e Encryption

5.8 HTTPS decryption and inspection on Cisco FTD, WSA and Umbrella

5.9 SMA for centralized content security management

5.10 Cisco advanced threat solutions and their integration: Stealthwatch, FMC, AMP, Cognitive Threat Analytics (CTA), Threat Grid, Encrypted Traffic Analytics (ETA), WSA, SMA, CTR, and Umbrella