5 Days

Cisco CCIE Security

The Cisco CCIE Security certification provides a career to security experts in managing and creating end-to-end secure networks by imparting the essential skills to architect, engineer, implement, troubleshoot, and support the full suite of Cisco security technologies and solutions.

The training will deploy the best industry best practices for teaching professionals to secure systems and environments against modern security risks, vulnerabilities, and requirements.

To earn the CCIE Security certification, a candidate must pass the following exam(s):

- 400-251 CCIE Security Written Exam
- CCIE Security Lab Exam v5.0

Course Details

Course Outline

1.0 Perimeter Security and Intrusion Prevention

1.1 Describing, Implementing, and troubleshooting HA features on Cisco ASA and Cisco FirePOWER Threat Defense (FTD)
1.2 Describing, Implementing, and troubleshooting clustering and routing protocols on Cisco ASA and Cisco FTD
1.3 Describing, Implementing, and troubleshooting different deployment modes
1.4 Describing, Implementing, and troubleshooting firewall features and IOS security features
1.5 Describing, Implementing, and troubleshooting Cisco Firepower Management Center (FMC) features and Cisco FTD deployment
1.6 Describing, Implementing, and troubleshooting correlation and remediation rules on Cisco FMC
1.7 Describing, Implementing, and troubleshooting Next Generation Firewall (NGFW) features
1.8 Describing, detecting, and mitigating common types of attacks

2.0 Advanced Threat Protection and Content Security

2.1 Comparing and contrasting different AMP solutions including public and private cloud deployment models
2.2 Describing, Implementing, and troubleshooting AMP for networks, AMP for endpoints, and AMP for content security (CWS, ESA, and WSA)
2.3 Detecting, analyzing, and mitigating malware incidents
2.4 Describing the benefits of threat intelligence provided by AMP Threat GRID
2.5 Perform packet capture and analysis using Wireshark, tcpdump, SPAN, and RSPAN
2.6 Describing, Implementing, and troubleshooting web filtering, user identification, and Application Visibility and Control (AVC)
2.7 Describing, Implementing, and troubleshooting mail policies, DLP, email quarantines, and SenderBase on ESA
2.8 Describing, Implementing, and troubleshooting SMTP authentication
2.9 Describing, Implementing, and troubleshooting SMTP encryption on ESA
2.10 Comparing and contrasting different LDAP query types on ESA
2.11 Describing, Implementing, and troubleshooting WCCP redirection
2.12 Comparing and contrasting different proxy methods

2.13 Describing, Implementing, and troubleshooting HTTPS decryption and DLP
2.14 Describing the security benefits of leveraging the OpenDNS solution.
2.15 Describing, Implementing, and troubleshooting SMA for centralized content security management
2.16 Describing the security benefits of leveraging Lancope

3.0 Secure Connectivity and Segmentation

3.1 Comparing and contrasting cryptographic and hash algorithms
3.2 Comparing and contrasting security protocols
3.3 Describing, Implementing and troubleshooting remote access VPN using technologies
3.4 Describing, Implementing, and troubleshooting the Cisco IOS CA for VPN authentication
3.5 Describing, Implementing, and troubleshooting clientless SSL VPN technologies with DAP and smart tunnels on Cisco ASA and Cisco FTD
3.6 Describing, Implementing, and troubleshooting site-to-site VPNs
3.7 Describing, Implementing, and troubleshooting uplink and downlink MACsec (802.1AE)
3.8 Describing, Implementing, and troubleshooting VPN high availability using Cisco ASA VPN clustering and dual-hub DMVPN deployments
3.9 Describing the functions and security implications of cryptographic protocols
3.10 Describing the security benefits of network segmentation and isolation
3.11 Describing, Implementing, and troubleshooting VRF-Lite and VRF-Aware VPN
3.12 Describing, Implementing, and troubleshooting micro-segmentation with TrustSec using SGT and SXP
3.13 Describing, Implementing, and troubleshooting infrastructure segmentation methods
3.14 Describing the functionality of Cisco VSG used to secure virtual environments
3.15 Describing the security benefits of data center segmentation using ACI, EVPN, VXLAN, and NVGRE

4.0 Identity Management, Information Exchange, and Access Control

4.1 Describing, Implementing, and troubleshooting various personas of ISE in a multi-node deployment
4.2 Describing, Implementing, and troubleshooting network access device (NAD), ISE, and ACS configuration for AAA
4.3 Describing, Implementing, and troubleshooting AAA for administrative access to Cisco network devices using ISE and ACS
4.4 Describing, Implementing, verify, and troubleshooting AAA for network access with 802.1X and MAB using ISE.
4.5 Describing, Implementing, verify, and troubleshooting cut-through proxy/auth-proxy using ISE as the AAA server
4.6 Describing, Implementing, verify, and troubleshooting guest life cycle management using ISE and Cisco network infrastructure
4.7 Describing, Implementing, verify, and troubleshooting BYOD on-boarding and network access flows with an internal or external CA
4.8 Describing, Implementing, verify, and troubleshooting ISE and ACS integration with external identity sources such as LDAP, AD, and external RADIUS
4.9 Describing ISE and ACS integration with external identity sources
4.10 Describing, Implementing, verify, and troubleshooting provisioning of AnyConnect with ISE and ASA
4.11 Describing, Implementing, verify, and troubleshooting posture assessment with ISE
4.12 Describing, Implementing, verify, and troubleshooting endpoint profiling using ISE and Cisco network infrastructure including device sensor
4.13 Describing, Implementing, verify, and troubleshooting integration of MDM with ISE
4.14 Describing, Implementing, verify, and troubleshooting certificate based authentication using ISE
4.15 Describing, Implementing, verify, and troubleshooting authentication methods
4.16 Describing the functions and security implications of AAA protocols
4.17 Describing, Implementing, and troubleshooting identity mapping on ASA, ISE, WSA and FirePOWER
4.18 Describing, Implementing, and troubleshooting 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 Describing, Implementing, and troubleshooting device hardening techniques and control plane protection methods.
5.3 Describing, Implementing, and troubleshooting management plane protection techniques
5.4 Describing, Implementing, and troubleshooting data plane protection techniques
5.5 Describing, Implementing, and troubleshooting IPv4/v6 routing protocols security
5.6 Describing, Implementing, and troubleshooting Layer 2 security techniques
5.7 Describing, Implementing, and troubleshooting wireless security technologies
5.8 Describing wireless security concepts
5.9 Describing, Implementing, and troubleshooting monitoring protocols
5.10 Describing the functions and security implications of application protocols
5.11 Describing the functions and security implications of network protocols
5.12 Describing the benefits of virtualizing security functions in the data center
5.13 Describing the security principles of ACI
5.14 Describing the northbound and southbound APIs of SDN controllers such as APIC-EM
5.15 Describing and identify key threats to different places in the network
5.16 Validate network security design for adherence to Cisco SAFE recommended practices
5.17 Describing Cisco Digital Network Architecture (DNA) principles and components.

6.0 Evolving Technologies

6.1 Cloud
6.2 Network Programmability (SDN)
6.3 Internet of Things (IoT)

Pre Requisite

- ?There are no specific prerequisites for CCIE certification.
- A candidate is expected to possess a thorough understanding of the exam topics and strongly encouraged to have three to five years of job experience before attempting certification.

Exams

CCIE Security Written Exam (350-018 CCIE Security) []

464, Udyog Vihar Phase V,Gurgaon (Delhi NCR)-122016,India	+91 8882 233 777	training@mercury.co.in	www.mercurysolutions.co

Date - May 03, 2025