CCIE Security

Introduction

Software and networking become more and more interconnected every day, creating an ever greater need for robust, scalable security across all platforms— from networks to mobile devices. And with intent-based networking, security teams can take advantage of automation to scale their security solutions. With CCIE Security certification, you can help lead these changes, and hiring managers know it: 71% of them say that certifications increase their confidence in an applicant's abilities.

CCIE Security certification helps you position yourself as a technical leader in the ever-changing landscape of security technologies and solutions. The certification covers core technology areas and validates your end-to-end lifecycle skills in complex security technologies and solutions from planning and design to operating and optimizing.

Exams and Recommended Training

1. 350-701 SCOR: Implementing and Operating Cisco Security Core Technologies

The Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0 course helps you prepare for the Cisco® CCNP® Security and CCIE® Security certifications and for senior-level security roles. In this course, you will master the skills and technologies you need to implement core Cisco security solutions to provide advanced threat protection against cybersecurity attacks. You will learn security for networks, cloud and content, endpoint protection, secure network access, visibility, and enforcement. You will get extensive hands-on experience deploying Cisco Firepower® Next-Generation Firewall and Cisco Adaptive Security Appliance (ASA) Firewall; configuring access control policies, mail policies, and 802.1X Authentication; and more. You will get introductory practice on Cisco Stealthwatch® Enterprise and Cisco Stealthwatch Cloud threat detection features.

This course, including the self-paced material, helps prepare you to take the exam, Implementing and Operating Cisco Security Core Technologies (350-701 SCOR), which leads to the new CCNP Security, CCIE Security, and the Cisco Certified Specialist - Security Core certifications.

Duration

5 Days

Course Objectives

- Describe information security concepts and strategies within the network
- Describe common TCP/IP, network application, and endpoint attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on Cisco ASA appliance and Cisco Firepower Next-Generation Firewall
- Describe and implement basic email content security features and functions provided by Cisco Email Security Appliance
- Describe and implement web content security features and functions provided by Cisco Web Security Appliance
- Describe Cisco Umbrella® security capabilities, deployment models, policy management, and Investigate console

- Introduce VPNs and describe cryptography solutions and algorithms
- Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco Firepower Next-Generation Firewall (NGFW)
- Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and Extensible Authentication Protocol (EAP) authentication
- Provide a basic understanding of endpoint security and describe Advanced Malware Protection (AMP) for Endpoints architecture and basic features
- Examine various defenses on Cisco devices that protect the control and management plane
- Configure and verify Cisco IOS software Layer 2 and Layer 3 data plane controls
- Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions
- Describe basics of cloud computing and common cloud attacks and how to secure cloud environment

Prerequisites

- Skills and knowledge equivalent to those learned in Implementing and Administering Cisco Solutions (CCNA®) v1.0 course
- Familiarity with Ethernet and TCP/IP networking
- Working knowledge of the Windows operating system
- Working knowledge of Cisco IOS networking and concepts
- Familiarity with basics of networking security concepts

Target Audience

- Cisco integrators and partners
- Consulting systems engineer
- Network administrator
- Network designer
- Network engineer
- Network manager
- Security engineer
- Systems engineer
- Technical solutions architect

Course Outline

- Describing Information Security Concepts*
  - Information Security Overview
  - Assets, Vulnerabilities, and Countermeasures
  - Managing Risk
- Describing Common TCP/IP Attacks*
  - Legacy TCP/IP Vulnerabilities
  - IP Vulnerabilities
  - Internet Control Message Protocol (ICMP) Vulnerabilities
- Describing Common Network Application Attacks*
  - Password Attacks
  - Domain Name System (DNS)-Based Attacks
  - DNS Tunneling
- Describing Common Endpoint Attacks*
  - Buffer Overflow
  - Malware
  - Reconnaissance Attack
- Describing Network Security Technologies
  - Defense-in-Depth Strategy

    - Defending Across the Attack Continuum
    - Network Segmentation and Virtualization Overview
- Deploying Cisco ASA Firewall
    - Cisco ASA Deployment Types
    - Cisco ASA Interface Security Levels
    - Cisco ASA Objects and Object Groups
- Deploying Cisco Firepower Next-Generation Firewall
    - Cisco Firepower NGFW Deployments
    - Cisco Firepower NGFW Packet Processing and Policies
    - Cisco Firepower NGFW Objects
- Deploying Email Content Security
    - Cisco Email Content Security Overview
    - Simple Mail Transfer Protocol (SMTP) Overview
    - Email Pipeline Overview
- Deploying Web Content Security
    - Cisco Web Security Appliance (WSA) Overview
    - Deployment Options
    - Network Users Authentication
- Deploying Cisco Umbrella*
    - Cisco Umbrella Architecture
    - Deploying Cisco Umbrella
    - Cisco Umbrella Roaming Client
- Explaining VPN Technologies and Cryptography
    - VPN Definition
    - VPN Types
    - Secure Communication and Cryptographic Services
- Introducing Cisco Secure Site-to-Site VPN Solutions
    - Site-to-Site VPN Topologies
    - IPsec VPN Overview
    - IPsec Static Crypto Maps
- Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs
    - Cisco IOS VTIs
    - Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 VPN Configuration
- Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
    - Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
    - Cisco ASA Point-to-Point VPN Configuration
    - Cisco Firepower NGFW Point-to-Point VPN Configuration
- Introducing Cisco Secure Remote Access VPN Solutions
    - Remote Access VPN Components
    - Remote Access VPN Technologies
    - Secure Sockets Layer (SSL) Overview
- Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW
    - Remote Access Configuration Concepts
    - Connection Profiles
    - Group Policies
- Explaining Cisco Secure Network Access Solutions
    - Cisco Secure Network Access
    - Cisco Secure Network Access Components
    - AAA Role in Cisco Secure Network Access Solution
- Describing 802.1X Authentication
    - 802.1X and Extensible Authentication Protocol (EAP)
    - EAP Methods
    - Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications
- Configuring 802.1X Authentication
    - Cisco Catalyst® Switch 802.1X Configuration
    - Cisco Wireless LAN Controller (WLC) 802.1X Configuration
    - Cisco Identity Services Engine (ISE) 802.1X Configuration
- Describing Endpoint Security Technologies*

    - Host-Based Personal Firewall
    - Host-Based Anti-Virus
    - Host-Based Intrusion Prevention System
- Deploying Cisco Advanced Malware Protection (AMP) for Endpoints*
    - Cisco AMP for Endpoints Architecture
    - Cisco AMP for Endpoints Engines
    - Retrospective Security with Cisco AMP
- Introducing Network Infrastructure Protection*
    - Identifying Network Device Planes
    - Control Plane Security Controls
    - Management Plane Security Controls
- Deploying Control Plane Security Controls*
    - Infrastructure ACLs
    - Control Plane Policing
    - Control Plane Protection
- Deploying Layer 2 Data Plane Security Controls*
    - Overview of Layer 2 Data Plane Security Controls
    - Virtual LAN (VLAN)-Based Attacks Mitigation
    - Spanning Tree Protocol (STP) Attacks Mitigation
- Deploying Layer 3 Data Plane Security Controls*
    - Infrastructure Antispoofing ACLs
    - Unicast Reverse Path Forwarding
    - IP Source Guard
- Deploying Management Plane Security Controls*
    - Cisco Secure Management Access
    - Simple Network Management Protocol Version 3
    - Secure Access to Cisco Devices
- Deploying Traffic Telemetry Methods*
    - Network Time Protocol
    - Device and Network Events Logging and Export
    - Network Traffic Monitoring Using NetFlow
- Deploying Cisco Stealthwatch Enterprise*
    - Cisco Stealthwatch Offerings Overview
    - Cisco Stealthwatch Enterprise Required Components
    - Flow Stitching and Deduplication
- Describing Cloud and Common Cloud Attacks*
    - Evolution of Cloud Computing
    - Cloud Service Models
    - Security Responsibilities in Cloud
- Securing the Cloud*
    - Cisco threat-centric Approach to Network Security
    - Cloud Physical Environment Security
    - Application and Workload Security
- Deploying Cisco Stealthwatch Cloud*
    - Cisco Stealthwatch Cloud for Public Cloud Monitoring
    - Cisco Stealthwatch Cloud for Private Network Monitoring
    - Cisco Stealthwatch Cloud Operations
- Describing Software-Defined Networking (SDN*)
    - Software-Defined Networking Concepts
    - Network Programmability and Automation
    - Cisco Platforms and APIs

Lab Outline

- Configure Network Settings and NAT on Cisco ASA
- Configure Cisco ASA Access Control Policies
- Configure Cisco Firepower NGFW NAT

- Configure Cisco Firepower NGFW Access Control Policy
- Configure Cisco Firepower NGFW Discovery and IPS Policy
- Configure Cisco NGFW Malware and File Policy
- Configure Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)
- Configure Mail Policies
- Configure Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Perform Endpoint Analysis Using AMP for Endpoints Console
- Explore File Ransomware Protection by Cisco AMP for Endpoints Console
- Explore Cisco Stealthwatch Enterprise v6.9.3
- Explore Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0
- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

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

The Cisco CCIE Security (v6.0) Practical Exam is an eight-hour, the 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 the exam topics below.

The following topics are general guidelines for the content likely to be included in 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.

Duration

8 Hours

Prerequisites

There are no formal prerequisites for CCIE Security, but you should have a good understanding of the exam topics before taking the exam.

CCIE candidates are recommended to have five to seven years of experience with designing, deploying, operating, and optimizing security technologies and solutions prior to taking the exam.

Course Outline

- Core Routing
  - Interior Gateway Protocol
    - IS-IS
    - OSPFv2 and OSPFv3

        - Optimize IGP scale and performance
        - IS-IS segment routing control plane for IPv4 and IPv6
        - OSPFv2 and OSPFv3 segment routing control plane
    - Border Gateway Protocol
        - IBGP, EBGP, and MP-BGP
        - BGP route policy enforcement
        - BGP path attribute
        - BGP scale and performance
        - BGP segments, BGP Labeled Unicast, and Linked State
    - Multicast
        - Design PIM (PIM-SM, PIM-SSM, and PIM-BIDIR)
        - Design RP (Auto-RP, BSR, Static, Anycast RP, and MSDP)
        - Design IGMP and MLD
        - MLDP
        - P2MP RSVP-TE
        - Tree-sid
    - Multiprotocol Label Switching
        - MPLS forwarding and control plane mechanisms
        - LDP
        - LDP scale and performance
        - SR (SRGB and Max Labels Depth)
        - LDP and SR Interworking - Segment routing mapping server
    - MPLS Traffic Engineering
        - ISIS and OSPF extensions
        - RSVP-TE
        - MPLS TE policy enforcement
        - MPLS LSP attributes
        - SR-TE
        - PCE and PCEP technology
        - Flexible Algorithm
        - Optimize MPLS TE scale and performance

- Architectures and Services
    - Virtualized Infrastructure
        - Design NFVI
        - Design Cloud scale networking Infrastructure
        - Design IaaS (Openstack) underlay architecture using Bare metal and Virtual Machines
        - Design convergence, virtual scaling, network Slicing, edge distribution, in 5G Architecture
    - Large scale MPLS Architecture
        - Unified MPLS
        - Multi-domain Segment Routing with SR-PCE
        - SLA based on IGP/TE metrics and Disjoint Paths
    - Carrier Ethernet
        - E-LINE, E-LAN, and E-TREE.
        - VPWS, VPLS, and H-VPLS
        - EVPN, EVPN-VPWS, EVPN-IRB
        - L2VPN service auto-steering into segment routing policy
    - L3VPN
        - L3VPN
        - Inter-AS L3VPN
        - Shared services, for example: Extranet and Internet access
        - L3VPN service auto-steering into segment routing policy
    - Internet service
        - IPv4 translation mechanism, for example: NAT44, CGNAT
        - IPv6 transition mechanism, for example: NAT64, 6RD, MAP, and DS Lite
        - Internet peering route and transit policy enforcement

  - Multicast VPN
    - Rosen mVPN
    - NG mVPN
  - Quality of Service for Core, Distribution, and Access
    - Classification and marking
    - Congestion management and scheduling
    - Congestion avoidance
    - MPLS QoS models (Pipe, Short Pipe, and Uniform)
    - MPLS TE QoS (MAM, RDM, CBTS, PBTS, and DS-TE)

- Access Connectivity
  - Layer-2 Connectivity
    - IEEE 802.1ad (Q-in-Q), IEEE 802.1ah (Mac-in-Mac), and ITU G.8032, REP
    - Spanning-Tree Access Gateway (MST-AG and PVST-AG)
    - Design and Operate MC-LAG
  - Layer-3 Connectivity
    - PE-CE routing protocols (OSPF, ISIS, and BGP)
    - Loop prevention techniques in multihomed environments

- High Availability and Fast Convergence
  - High Availability
    - (SS0/NSF, NSR, and GR)
  - Routing/fast convergence
    - IGP convergence
    - LDP convergence
    - BGP convergence - Prefix Independent Convergence (BGP-PIC)
    - BFD
    - LFA-FRR (LFA, Remote LFA, and TI-LFA)
    - MPLS TE FRR

- Security
  - Control plane security
    - Control plane protection techniques (LPTS and CoPP)
    - Routing Protocol and LDP authentication and security
    - BGP prefix-based and attribute-based filtering
    - BGP-RPKI (Origin AS validation)
  - Management plane security
    - Implement and troubleshoot device management (MPP, SSH, and VTY)
    - Implement and troubleshoot logging and SNMP security
    - Implement and troubleshoot AAA
  - 5.3 Infrastructure security
    - ACL
    - uRPF
    - RTBH and Router Hardening
    - BGP Flowspec

- Assurance and Automation
  - Network Assurance
    - Syslog and logging functions
    - SNMP traps and RMON
    - NetFlow and IPFIX
    - Segment Routing OAM and MPLS OAM
    - Segment Routing Data Plane monitoring
    - IP/MPLS Performance monitoring (TCP, UDP, ICMP, and SR)
    - Ethernet OAM (Y.1564 and Y.1731)
  - Network Automation
    - Design, deploy and optimize NSO service packages (Yang model, template-based, python-based, fast map, reactive fast map, CLI NEDs,

- NETCONF NEDs, NSO northbound integration using REST and RESTCONF).
- Design NFV orchestration (NFVO) using NSO and ESC in an ETSI NFV architecture.
- Design and deploy Model-driven telemetry on XR devices (Yang models, gRPC, GPB, device configuration, collection architecture)
- Deploy and Optimize Ansible playbook scripts that interact with NSO, IOS-XE, and IOS-XR devices