CCIE Security Certification (Exam 400-251) (Coming Soon)

Modality: On Demand

Duration:

This course is for professionals planning to enroll in the 400-251 CCIE Exam leading to the 400-251 CCIE Certification. The official exam voucher is not included in this course. However, the official exam voucher can be purchased separately on request.

About this Course:

This CCIE Security training program is designed for professionals who want to nurture the skills of creating, engineering, troubleshooting, and deploying security solutions. The primary objective of this course is to train professionals and candidates for excellence in the 400-251 CCIE Certification Written and Lab Exam. The following three courses are designed to help candidates develop a sound knowledge of the exam topics: SASAC, SASAA, and ASA Lab Camp.

Course Objectives:

The core objective of this course is to help professionals gain a better understanding and sound knowledge of the following key concepts:

- Cisco ASA 5500 X Series Next-Gen Firewalls Fundamentals
- Connectivity Management and Cisco ASA Policy Controls
- Cisco ASA VPN Components and Basic Device Implementation
- Cisco ASA Clientless Solution Implementation for VPN
- Cisco ASA and AnyConnect VPN Solution Implementation
- Cisco ASA Identity Firewall Security Policies
- Configuring Cisco Firepower Service Module
- Cisco ASA Cloud Web Security and Clustering Implementation
- Security Group Firewalls and Cisco Change of Authorization Essentials

Job Roles:

Certified Cisco Security Professionals can follow a career path to Certified Cisco Internet Security Experts and can pursue the following careers:

- Network Security Administrators – Average Annual Salary $68,156
- Network Security Specialist – Average Annual Salary $74,000
- Network Security Engineer – Average Annual Salary $84,000

Audience:

- Network Engineers and Managers
- Network Designers and Administrators

- Professionals working with Cisco ASA9.X
- Professionals liable for maintaining, monitoring, and deploying network security

Prerequisites:

There are no obligatory prerequisites for this course and any interested candidate and professional can enroll in this course. However, there are prerequisites of the 400-251 CCIE Certification Exam:

- Basic Knowledge and Know-how of Certification Exam Topics
- Minimum 3 to 5 Years Practical Experience is Highly Recommended
- Clearing the Theoretical Exam is mandatory to attempt the Security Practical Exam

Course Outline:

SASAC

Module 1: Cisco ASA Adaptive Security Appliance Essentials

- Evaluating Cisco ASA Adaptive Security Appliance Technologies
- Identifying Cisco ASA Adaptive Security Appliance Models
- Identifying Cisco ASA Adaptive Security Appliance Licensing Options

Module 2: Basic Connectivity and Device Management

- Preparing the Cisco ASA Adaptive Security Appliance for Network Integration
- Managing Basic Cisco ASA Adaptive Security Appliance Network Settings

Module 3: Network Integration

- Configuring Cisco ASA Adaptive Security Appliance NAT Features
- Configuring Cisco ASA Adaptive Security Appliance Basic Access Control Features
- Configuring Cisco ASA Adaptive Security Appliance Routing Features

Module 4: Cisco ASA Adaptive Security Appliance Policy Controls

- Defining the Cisco ASA Adaptive Security Appliance MPF
- Configuring Cisco ASA Adaptive Security Appliance Advanced Application Inspections

Module 5: Cisco ASA Adaptive Security Appliance VPN Common Components

- VPN Overview
- Implementing Profiles, Group Policies, and User Policies
- Implementing PKI Services

Module 6: Cisco Clientless VPN Solution

- Introducing Clientless SSL VPN

- Deploying Basic Cisco Clientless SSL VPN on the Cisco ASA Adaptive Security Appliance
- Deploying Application Access in Cisco Clientless SSL VPN
- Deploying Client-Side Authentication and Authorization in Clientless SSL VPN

Module 7: Cisco AnyConnect Full Tunnel VPN Solutions

- Deploying Basic Cisco AnyConnect SSL VPN on Cisco ASA
- Deploying Advanced Cisco AnyConnect SSL VPN on Cisco ASA
- Deploying Advanced Authentication and Authorization in Cisco AnyConnect VPNs
- Deploying Cisco AnyConnect IPsec/IKEv2 VPNs

Module 8: Cisco ASA Adaptive Security Appliance High Availability and Virtualization

- Configuring Cisco ASA Adaptive Security Appliance Interface Redundancy Features
- Configuring Cisco ASA Adaptive Security Appliance Active/Standby High Availability
- Configuring Security Contexts on the Cisco ASA Adaptive Security Appliance
- Configuring Cisco ASA Adaptive Security Appliance Active/Active High Availability (Optional/Self-study)

Lab

- Accessing the Remote Lab Environment
- Configuring the Cisco ASA Adaptive Security Appliance
- Configuring NAT
- Configuring Basic Cisco Access Control Features
- Configuring MPF, Basic Stateful Inspections, and QoS
- Configuring MPF Advanced Application Inspections
- Implementing Basic Clientless SSL VPN on the Cisco ASA
- Configuring Application Access for Clientless SSL
- VPN on the Cisco ASA
- Implementing External Authentication and Authorization for Clientless SSL VPNs
- Implementing Basic Cisco AnyConnect SSL VPN on the Cisco ASA
- Configuring Advanced Authentication for Cisco AnyConnect SSL VPNs
- Implementing Cisco AnyConnect IPsec/IKEv2 VPNs
- Configuring Active/Standby High Availability

SASAA

Module 1: Cisco ASA Product Family

- Introduction to ASA series firewalls
- Introduction to ASAv
- Deploy ASAv
- ASAv Other hypervisors support, digitally signed image and management options
- Verify ASAv VM
- ASA 9.2.1 BGP IPv6 support
- ASA 9.3 features

- ASA 9.4.1 + VXLAN support
- Describe the Cisco ASASM platforms, architecture, and features

Module 2: Cisco ASA Identity Firewall

- ASA Identity Firewall benefits, flow and policies
- Cisco CDA basic network configuration
- Application status verification
- Active directory server configuration
- CDA user-account configuration
- CDA GUI password policy configuration
- Configure identity firewall policies on ASA
    - Using ASDM
    - Using CLI
- FQDN network object configuration
- Verify user-identity operations
- CDA management with CLI, live log monitoring and troubleshooting

Module 3: Cisco ASA Firepower Services

- SFR introduction
- FireSIGHT management
- SFR management interface, package installation and verification
- FireSIGHT VM installation and setup
- License requirement
- Policy types introduction
- Recommended rules introduction
- Monitoring
- ASDM and Firepower on-box FireSIGHT manager
- Firepower dashboard, reporting, status and events viewer
- Licensing
- Firepower 6.0 features
- System configurations and device platform settings
- Firepower multidomain management

Module 4: Cisco ASA Cloud Web Security (CWS)

- ASA with CWS introduction
- CWS scanning processes
- Licenses
- ASA with CWS integration
- CWS operations verification
- Verify traffic redirection
- Syslog messages
- ScanCenter web filtering policy introduction and configuration
- ASA CWS AMP introduction
- CWS cognitive threat analysis
- Threats reporting

Module 5: Cisco ASA Clustering

- Cluster performance figures and supported platforms
- Cluster data-interface modes and connections
- CLL functions
- Cluster dynamic-routing, NAT and PAT operations
- Cluster terminology
- TCP, asymmetric UDP, short-lived and centralized-feature traffic flows
- Cluster management
- Configuration with the CLI
- Each unit configuration
- Master unit configuration
- Sample configuration of a two-unit cluster with spanned etherchannel and individual interface
- Configure ASA cluster using Cisco ASDM
- Cluster licensing
- Verification types
- Troubleshoot ASA cluster operations
- Cluster features of v9.1.4, v9.2.1, v9.3.1 and v9.4.1

Module 6: Cisco ASA Security Group Firewall and Change of Authorization (Optional)

- Cisco secure access architecture
- SG Firewall configuration
- SGACL operations monitoring
- SGT features (post 9.0 releases)
- Change of authorization introduction
- Chang of authorization CLI and ASDM configurations

Labs:

- Access the Remote Cisco Learning Lab Environment
- Set Up and Test the ASAv
- Implement New Features in ASA 9.3 and 9.4
- Configure the Cisco CDA
- Configure ASA IDFW
- Cisco ASA Firepower Services Module Installation
- Cisco Firepower Management Center Configuration
- Configure ASA CWS
- Cisco ASA Cluster Configuration