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

Modality: Self-Paced Learning

Duration: No

SUBSCRIPTION: Learn, Master, Master Plus

About this course:

The Cisco Certified Internetwork Expert Security (CCIE Security) program recognizes security experts who have the knowledge and skills to architect, engineer, implement, troubleshoot, and support the full suite of Cisco security technologies and solutions using the latest industry best practices to secure systems and environments against modern security risks, threats, vulnerabilities, and requirements.

To earn CCIE Security certification, you must not only prove your theoretical knowledge of security best practices in the CCIE Security written exam, but you must also demonstrate your skill in the CCIE Security lab exam using real equipment in real-world scenarios. Because of this rigorous process and the expert-level knowledge and skill it requires, CCIE Security certification is one of the most advanced network security certifications available and qualifies you to manage, lead, and design the most complex network security teams and projects.

This certification path will act as exam prep for two exams, CCIE Security Written Exam (?400-251), and CCIE Security Lab Exam (Lab 5.0).

This certification path contains the following courses:

SASAC - Implementing Core Cisco ASA Security is the first of two courses that acts as the **exam prep** for the written 400-251. This enhanced course contains added depth to the standard labs, using a topology that simulates a typical production network. You'll use ASA 5515 appliances to work through configuring access control to and from your network.

Additionally, the PC systems and server systems are an integral part of the lab environment. Here you will use Windows 8, Windows Server 2012, and Kali Linux to manage, test, and even attack your lab network using real-world operating systems and applications.

SASAA - Implementing Advanced Cisco ASA Security is the second of two courses that acts as the **exam prep** for the written **400-251.** This course provides advanced training on the key Cisco Adaptive Security Appliance (ASA) 9.x features including the following:

- Cisco ASA 5500-X Series Next-Generation Firewalls, ASAv, ASA 5506-X, 5508-X, 5516-X and ASA SM and implement new ASA 9.4.1 features
- Cisco ASA Identity Firewall policies
- Install and Set up the Cisco FirePOWER Services Module (SFR)
- Implement Cisco ASA Cloud Web Security
- Implement a Cisco ASA cluster
- Cisco ASA security group firewall and change of authorization support

ASA Lab Camp is the last course in this certification path. This course will act as exam prep material for the **CCIE Security lab exam**. The CCIE Security lab exam is an eight-hour, hands-on exam which requires you to configure a series of secure networks to given specifications. Knowledge of troubleshooting is an important skill, and you are expected to diagnose and solve issues as part of the CCIE Security lab exam. You must pass the lab exam within three years of passing the written exam to achieve CCIE Security certification. Your first lab attempt must be made within 18 months.

This exclusive, lab-based course, provides you with your own set of equipment, giving you the Adaptive Security Appliance (ASA) 9.x and ASA SFR-based lab experience in just five days. This course provides 29 different lab scenarios using Cisco equipment such as: ASA v9.5, ASA 5515-X NGFW (Next-Generation Firewall SFR), Access Control Server (ACS 5.4), Context Directory Agent (CDA), Catalyst switch, Integrated Services Router (ISR), and ASA 55x5.

Course Objective:

By the end of this course, you should be able to:

- Explain the core essential features of Cisco ASA 5500-X Series Next-Generation Firewalls
- Describe how to implement Cisco ASA basic connectivity and device management
- Implement basic Cisco ASA network integration
- Describe and implement basic Cisco ASA policy controls
- Describe Cisco ASA common VPN components
- Describe and implement Cisco ASA clientless VPN solutions
- Describe and implement Cisco ASA and Cisco AnyConnect full tunnel VPN solutions
- Describe the Cisco ASA 5500-X Series Next-Generation Firewalls, ASAv, ASA 5506-X, 5508-X, 5516-X, and ASASM and implement new ASA 9.4.1 features
- Implement Cisco ASA Identity Firewall policies
- Install and set up the Cisco Firepower Services Module (SFR)
- Implement Cisco ASA Cloud Web Security
- Implement cisco ASA Clustering
- Describe Cisco ASA Security Group Firewall and Change of Authorization Support

Job Roles associated with the Cisco Certified Internetwork Expert Security:

- Network security engineer **USD 84,000**
- Network security administrator **USD 68,156**
- Network security specialist **USD 74,000**

Audience:

Due to a growing cyber-criminal underworld, network security is becoming a top priority for the modern business. And as the demand for strict security software increases, so too does the need for network engineers able to implement a variety of security software to scale. That’s why this class is ideal for network engineers, network managers, network designers, network administrators and any other IT personnel tasked with maintaining, implementing and/or monitoring a company’s network security.

The primary audience for this course is as follows:

- Network engineers supporting Cisco ASA 9.x implementations

Prerequisite:

- There are no formal prerequisites for CCIE certification. Prior professional certifications or training courses are not required. As a CCIE Security candidate, you must first pass the written qualification exam and then the corresponding hands-on lab exam. You are expected to have an in-depth understanding of the exam topics and strongly encouraged to have three to five years of job experience before attempting certification.

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