CCIE Security

400-251 CCIE Security Written Exam

The written exam is a two-hour test with 90–110 questions that validate experts who have the knowledge and skills needed to architect, design, engineer implement, operate, and troubleshoot complex security technologies and solutions. Candidates must understand network security requirements, how different components and systems interoperate, and translate these security requirements into device configurations. The exam is closed book and no outside reference materials are allowed.

The 400-251 CCIE Security written exam validates 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.

Topics include network functionality and security-related concepts and best practices, as well as Cisco network security products, solutions, and technologies in areas such as next generation intrusion prevention, next generation firewalls, identity services, policy management, device hardening, and malware protection.

The written exam utilizes the unified exam topics which includes emerging technologies, such as Cloud, Network Programmability (SDN), and Internet of Things (IoT).

CCIE Security Lab Exam v5.0

Lab Exam v5.0 Overview

The Cisco CCIE Security Lab Exam version 5.0 is an eight-hour, hands-on exam that requires a candidate to plan, design, implement, operate, and troubleshoot complex security scenarios for a given specification. Knowledge of troubleshooting is an important skill and candidates are expected to diagnose and solve issues as part of the CCIE lab exam.

CCIE Security v5.0 unifies written and lab exam topics documents into a unique curriculum, while explicitly disclosing which domains pertain to which exam, and the relative weight of each domain.

Lab Format

The eight-hour lab format consists of three modules and need to be taken in the following sequence during the day of the exam:

Module 1: Troubleshooting module (two hours)

The Troubleshooting module delivers incidents that are independent of each other, which means that the resolution of one incident does not depend on the resolution of another. The topology that is used in the Troubleshooting module is different than the topology used in the Configuration module.

The Troubleshooting module is 2 hours. If desired, candidates can extent the Troubleshooting module's time by borrowing up to 30 min from the Configuration module. Note, the total Configuration's module time will be reduced by the extra time spend in the Troubleshooting module (if any, up to 30 min). If candidates finish the Troubleshooting module early, the unused Troubleshooting module's time will be added to the Configuration module's time, ensuring a total lab exam time of 8 hours. The Diagnostic module is fixed in duration (60 minutes).

Module 2: Diagnostic module (one hour)

The new Diagnostic module focuses on the skills required to properly diagnose network issues, without having device access. Candidates will be provided with a set of documentation that represents a snapshot of a realistic situation: at a point in time in an investigation process that a network engineer might be facing. The main objective of the Diagnostic module is to assess the skills required to properly diagnose network issues. These skills include:

- Analyze
- Correlate: Discerning multiple sources of documentation (such as e-mail threads, network topology diagrams, console outputs, logs, and even traffic captures.)

These activities are naturally part of the overall troubleshooting skills. They are designed as a separated lab module because the format of the items is significantly different. In the Troubleshooting module, the candidate needs to be able to troubleshoot and resolve network security issues on actual devices.

In the Diagnostic module, the candidate need to make choices between pre-defined options to either indicate:

- What the root cause of the issue is?
- Where is the issue located in the diagram?
- What critical piece of information allows you to identify the root cause?
- What missing piece of information allows you to identify the root cause?

Module 3: Configuration module (five hours)

The Configuration module provides a setup very close to an actual production network having various security components providing various layers of security at different points in the network. Though the major part of the module is based on virtual instances of the Cisco security appliances, the candidate may be asked to work with physical devices as well. At the beginning of the module, the candidate has full visibility of the entire module. A candidate can choose to work in the sequence in which the items are presented or can resolve items in whatever order seems preferable and logical.