Cisco CCIE Security Certification Written and Lab Content Updates

The Cisco CCIE Security exam topics have been refreshed from v4.0 to v5.0. The new exam curriculum comprises six domains. The new segmentation into these six domains was done to improve the logical structure of the topics and to align them with Cisco's security solutions portfolio.

Each domain lists the tasks that a minimally qualified candidate should be able to perform. Please note that the topics in the exam serve as a general guideline for the content likely to be included in the exam. Other related topics may also appear on any delivery of the exam. All domains and their tasks can appear in both the written and lab exams, making for unified exam topics.

Domain Comparison of CCIE Security Exam v4.0 and v5.0

Below is the domain-level comparison of CCIE Security exams v4.0 and v5.0.

CCIE Security Written Exam Topics v4.0	CCIE Security Unified Exam Topics v5.0
1.0 Infrastructure, Connectivity, Communications, and Network Security	1.0 Perimeter Security and Intrusion Prevention
2.0 Security Protocols	2.0 Advanced Threat Protection and Content Security
3.0 Application and Infrastructure Security	3.0 Secure Connectivity and Segmentation
4.0 Threat Vulnerabilities Analysis and Mitigation	4.0 Identity Management , Information Exchange, and Access
5.0 Cisco Security Products, Features, and Management	5.0 Infrastructure Security, Virtualization, and Automation
6.0 Cisco Security Technologies and Solutions	6.0 Evolving Technologies
7.0 Security Policies and Procedures, Best Practices, and Standard	
8.0 Evolving Technologies *(this domain was only included in the Written exam topics v4.1)*	
CCIE Security Lab Exam Topics v4.0	
1.0 System Hardening and Availability	
2.0 Threat Identification and Mitigation	
3.0 Intrusion Prevention and Content Security	
4.0 Identity Management	
5.0 Perimeter Security and Services	
6.0 Confidentiality and Secure Access	

Compared to v4.0, the domains were renamed, reshuffled, and combined to focus more on technologies than on hardware and to create a logical structure from the perspective of security solutions deployment. The v5.0 exam

introduces the latest technologies and solutions, such as NGIPS, AMP, APIC-EM, and information exchange, to keep the new unified exam topics relevant to the cutting-edge customer-based production deployment.

NOTE: Even though Domain 7 in v4.0 (Security Policies and Procedures, Best Practices, and Standards) is not specifically called out in the new exam, it is now part of Domain 5 in v5.0 (Infrastructure Security, Virtualization, and Automation).

CCIE Security Exam Changes

The decision to add or remove any task was based on the feedback received from security subject matter experts during the job role analysis and job task analysis of the v5.0 exam. Any variations in v5.0 topics from v4.0 reflect both the evolving network security environment and security job roles in the market.

Topics Removed from v4.0	Topics Added in v5.0
Legacy IPS Appliance	Advanced Threat Protection
Cisco Easy VPN	Virtualization
	Automation
	Information Exchange
	Evolving Technologies

For the v5.0 lab exam, the hardware and software have been updated with significant virtualization of Cisco security appliances. The written exam may present questions based on the virtual instance as well the physical hardware of Cisco security appliances.

Below is a comparison of hardware and software changes from v4.0 to v5.0.

CCIE Security Hardware and Software v4.0	CCIE Security Hardware and Software v5.0
Hardware	**Virtual Machines**
Routers · ISR 3825: 15.1(3)T3 · ISR 1841: 15-2.T1 · ISR 2951-G2: 15.1(3)T3	Security Appliances · Cisco Identity Services Engine (ISE): 2.1.0 · Cisco Secure Access Control System (ACS): 5.8.0.32 · Cisco Web Security Appliance (WSA): 9.2.0 · Cisco Email Security Appliance (ESA): 9.7.1 · Cisco Wireless Controller (WLC): 8.0.133 · Cisco Firepower Management Center Virtual Appliance: 6.0.1 and/or 6.1 · Cisco Firepower NGIPSv: 6.0.1 · Cisco Firepower Threat Defense: 6.0.1
Catalyst Switches · 3560-E: 122-55.SE5 · 3750-X: 150-1.SE2	Core Devices · IOSvL2: 15.2 · IOSvL3: 15.5(2)T · Cisco CSR 1000V Series Cloud Services Router: 3.16.02.S · Cisco Adaptive Security Virtual Appliance (ASAv): 9.6.1
ASAs · 5512-X: 8.6(1) · 5510: 8.4(3),8.2(5)	Others · Test PC: Microsoft Windows 7 · Active Directory: Microsoft Windows Server 2008 (AD is not required to be configured by the candidate) · Cisco Application Policy Infrastructure Controller Enterprise Module : 1.2 · Cisco Unified Communications Manager: (The CUCM is not required to be configured by the candidate) · FireAMP Private Cloud · AnyConnect 4.2

IPS · 4240: 7.0(7)E4	**Physical Devices**
WSA · S170: 7.1.3-021	Cisco Catalyst Switch · C3850-12S: 16.2.1
WLC · 2504: 7.2.103.0	Cisco Adaptive Security Appliance · 5512-X: 9.6.1
AP · 1242G: 124-25e	Cisco 2504 Wireless Controller · 2504: 8.0.133.0
Virtual Machines	Cisco Aironet · 1602E: 15.3.3-JC
· ISE: 1.1.1 · ACS: 5.3 · Test PC: Windows 7 · AD: Windows Server 2008	Cisco Unified IP Phone · 7965: 9.2(3) (IP Phone is not required to be configured by the candidate)

Unified Exam Topics

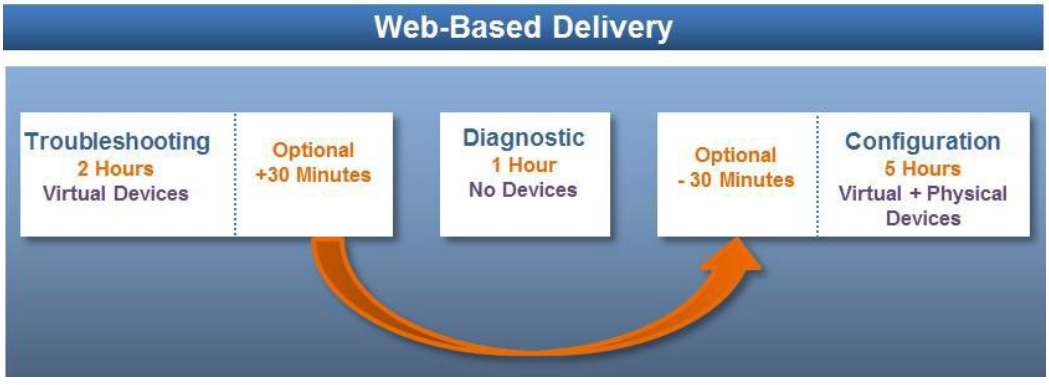
The CCIE Security v5.0 exam unifies the written and lab exam topics into a unique curriculum, while explicitly disclosing which domains pertain to which exam, with their relative weight distribution.

CCIE Security Written Exam v5.0 Format

The written exam number has changed from 350-081 to 400-251. The exam will include a new educational approach ensuring that Expert-level candidates demonstrate knowledge and skills with evolving technologies such as network programmability, cloud, and the Internet of Things. The intent is to ensure that certified experts are well equipped to participate in meaningful discussions with business leaders about these new technical areas that greatly influence businesses globally.

CCIE Security Lab Exam v5.0 Format

The web-based delivery infrastructure supporting the v5.0 lab exam is very similar to v4.0. The format of the lab exam itself, however, has changed significantly. The v5.0 lab exam now comprises three modules.



- **Troubleshooting Module**

  The Troubleshooting module delivers incidents that are independent of each other, meaning 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 from the topology that is used in the Configuration module.

  The Troubleshooting module is two hours long; however, the candidate can borrow up to 30 minutes from the five hours allotted to the Configuration module. In other words, the candidate can choose to use an extra 30 minutes for either the Troubleshooting module or the Configuration module.

- **Diagnostic Module**

  The new Diagnostic module is one hour long, and its main objective is to assess the skills required to properly diagnose network issues without having device access. These skills include the following:

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

  These activities are naturally part of overall troubleshooting skills. They are designed as a separate 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 needs to make choices from among predefined options:

  - What is the root cause of the issue?
  - 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?

- **Configuration Module**

  The Configuration module provides a setup very close to an actual production network having security components providing various layers of security at various points in the network.

  Though the major part of the module is based on virtual instances of Cisco security appliances, the candidate may be asked to work with the physical devices as well.

  At the beginning of a 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.

  The modules in the lab exam are delivered in a fixed sequence: the Troubleshooting module, followed by the Diagnostic module, and lastly, the Configuration module. The entire lab exam is up to eight hours long.

  It is important to note that the system does not allow the candidate to go back and forth between modules. When working in the Troubleshooting module, the candidate can choose to use an extra 30 minutes in addition to the two hours allotted to complete the module. However, the candidate cannot see the

Configuration module at that point and cannot know where the extra time will be needed more. The total exam time is eight hours, so using the extra 30 minutes for the Troubleshooting module, means that the candidate will have only four and a half hours to complete the Configuration module. If the candidate spends only two hours on the Troubleshooting module, the Configuration module is credited by the time gained, so the candidate then has five hours to complete that module.

The web-based delivery system displays a warning message when the allotted two hours has expired in the Troubleshooting module. The system asks whether the candidate wants to continue working on the Troubleshooting module (if so, adding up to 30 extra minutes before advancing to the next module) or wants to stop working on the Troubleshooting module and advance to the Diagnostic module.

The Diagnostic module does not have terminal sessions to access the device console. This module provides the candidate with a set of documentation that represents a snapshot of a realistic situation: a point in time in an investigation that a network engineer might be facing. For example, a support engineer might need to provide a root cause analysis to a customer, help a colleague who is stuck in a troubleshooting process, or summarize the previous investigation steps.

Within the Diagnostic module, the items are presented in a format that is similar to the written exam. It includes these formats:

- Multiple choice (single answer or multiple answers)
- Drag-and-drop
- Point and click diagrams

The Diagnostic module questions (called troubleshoot tickets) contain a set of documentation that the candidate must consult to understand the problem scenario. Then the candidate analyzes and correlates information (after distinguishing between valuable and worthless information) to make a correct choice from among the predefined options listed in the item.

The troubleshoot tickets do not require candidates to write anything to provide the answer. All tickets are close-ended; in other words, the grading is deterministic, which ensures fair and consistent scoring. This approach also helps to grant credit to candidates who accurately identify the root cause of a networking issue but fail to resolve it within the defined constraints, which the Troubleshooting module does not offer.

Real-life experience is certainly the best training to prepare for the module. Candidates with limited experience should focus on discovering, practicing, and applying the efficient and effective troubleshooting methodologies that are used for any realistic networking challenge.

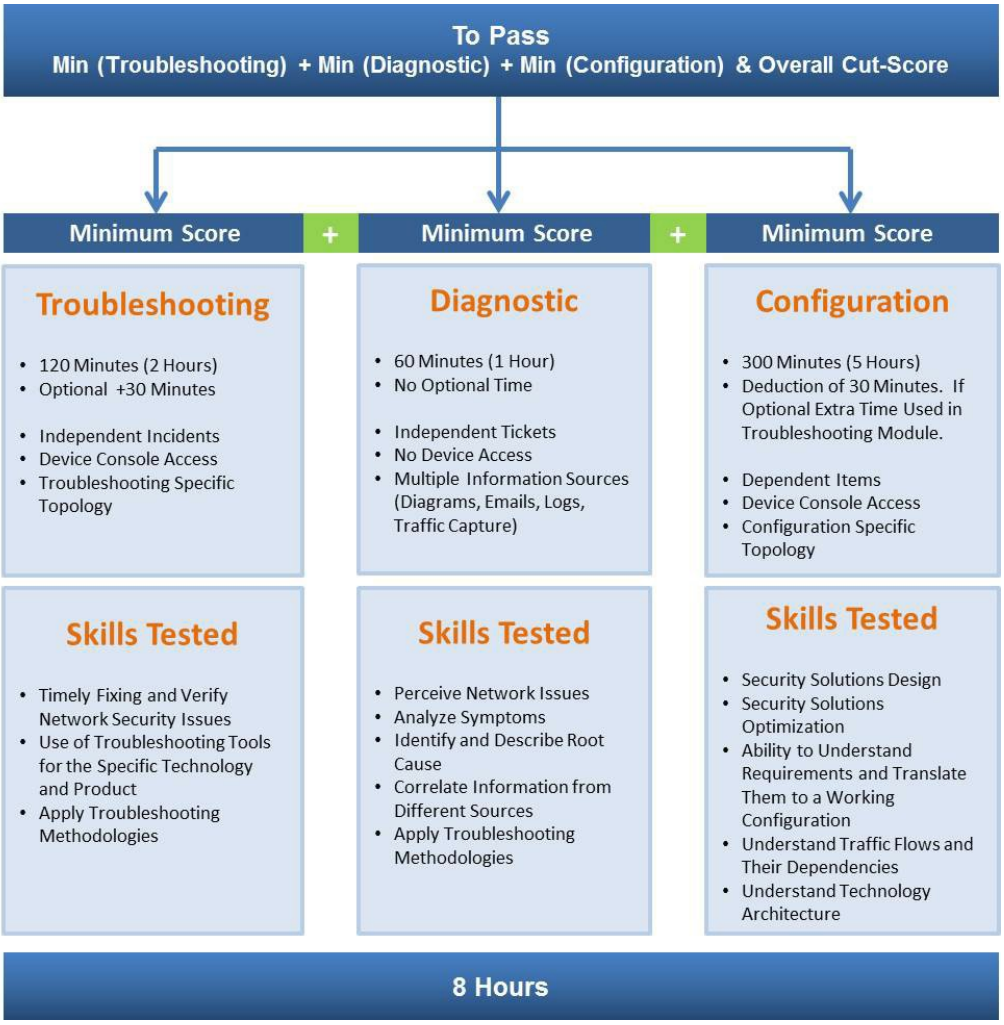
Passing Criteria

To pass the lab exam, the candidate must meet these two conditions:

- The total sum of all of modules must equal at least the minimum overall cut score.
- The sum for each individual module must equal at least the minimum cut score for the module.

These criteria prevent the candidate from passing the lab exam while failing or even bypassing a module; for example, the Diagnostic module.

The point value of each item in each lab module is shown on the candidate guide, which is provided at the lab exam. The points are granted only when all the criteria of the item are met. No partial score is granted on any item.



Learn More

Get more information on the CCIE Security Certification.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 06/16