Cisco CCIE Security
Exam Preparation Tips

This article highlights some of the important aspects about the Cisco CCIE® Security exam and provides valuable tips to prepare for taking the exam.

Planning Resources

With the ever-growing proliferation of the Internet and mass information sharing across shared communities, there is an abundance of preparation materials available to help you prepare for the Cisco CCIE Security certification exams. However, be selective and choose preparation materials that offer a hands-on, pragmatic approach that allows you to exercise your configuration and troubleshooting skills.

Assessing Strengths and Weaknesses

There is no single, universal formula or recipe for CCIE preparation. Candidates have their own strengths and weaknesses, and they should know how to capitalize on those strengths and minimize those weaknesses.

- Use the blueprints (written and lab) to determine your conceptual, theoretical, and practical experience and to establish a skill matrix. Identify your knowledge level by rating yourself on each topic, using a scale of 1 to 5 (with 1 being poor, and 5 being excellent).
- Evaluate your hands-on experience in each technology and topic area listed on the blueprint (lab exam).
- For areas of strength, practice for speed and perfection.
- For weaker areas, boost your knowledge with training, books, online resources, and much hands-on practice.

Using your skill matrix just mentioned, draw your own unique study plan and customize it to reflect your personal technological strengths and weaknesses. *A good study plan is integral to your CCIE success!*

Here are links to the necessary blueprints:

CCIE Security Written Exam Blueprint:
http://www.cisco.com/web/learning/le3/ccie/security/wr_exam_blueprint_v2.html

CCIE Security Lab Exam Blueprint:
http://www.cisco.com/web/learning/le3/ccie/security/lab_exam_blueprint_v2.html

Trainings

An important note to keep in mind is that training is not a prerequisite or formal requirement to achieve CCIE certification. However, these training courses are recommended and are listed at http://www.cisco.com/web/learning/le3/ccie/security/training.html:

- Securing Networks with Cisco Routers and Switches (SNRS)
- Securing Cisco Network Devices (SND)
- Securing Networks with PIX and ASA (SNPA)
- Cisco Secure Virtual Networks (CSVPN)
- Implementing Cisco Intrusion Prevention System (IPS)
- Securing Hosts Using Cisco Security Agent (HIPS)

In addition to these training courses, there are numerous *FREE* online Cisco Quick Learning Training Modules readily available. Candidates can use these web-based modules at their convenience. Here is a sample of the modules that candidates might find helpful:

- Configuring Cisco ASA and Cisco PIX security appliances
  http://www.cisco.com/web/learning/le31/le29/configuring_asa_pix_security_appliances.html
  - Utilizing the Packet Tracer Feature on the Cisco ASA
  - Simplifying Access Control Policies on PIX 500 and ASA 5500
  - Configuring the Easy VPN Hardware Client feature on the Cisco ASA 5505
  - Configuring the L2TP/IPSEC Feature on the Cisco ASA
  - Using Cisco ASA 5500 Series SSL VPN for Clientless Access (WebVPN)
  - SSL VPN Client Access on ASA 5500
  - VPN Clustering for ASA 5500
  - Modular Policy Framework on PIX 500 and ASA 5500
  - Active/Active Failover for ASA 5500
  - Active/Standby Failover for ASA 5500
  - Configuring Basic Features on the Cisco ASA 5505

- Configuring Cisco IPS 4200 Series Sensors
  http://www.cisco.com/web/learning/le31/le29/configuring_ips_4200_series_sensors.html
  - Understanding and Configuring In-Line VLAN IPS
  - Understanding and Configuring In-Line IPS
  - Configuring Event Action Rules
  - Configuring the Meta Event Generator

- Security and VPN Quick Learning Modules
  - Securing Cisco LAN Switches (SECL) 1.0
  - Securing Cisco Routers (SECR) v1.0

Links to all of these trainings and more, including courses and online learning modules, can be found at http://www.cisco.com/web/learning/le3/ccie/security/training.html.

Additionally, there are many miscellaneous IP Routing learning modules. Please note that routing and switching are preconfigured in the CCIE Security lab exam; however, candidates need to have knowledge of these areas in order to understand and troubleshoot any possible underlying problems. Therefore, it is highly recommended that you take advantage of some of the educational resources available at http://www.cisco.com/web/learning/le31/le29/learning_recommended_training_routing_switching.html.

CCIE "Boot Camps"

Many third-party vendors offer training sessions and preparation workshops, known as "boot camps," that are sometimes of interest for CCIE candidates. Please note that these training sessions do not use curriculum authorized by Cisco, and the CCIE team does not officially endorse them. Whether or not to attend such a boot camp to prepare for CCIE certification is at the sole discretion of the candidate.

In general, boot camps provide mock scenarios that help candidates gauge their exam readiness and provide the candidate with essential tips for exam taking. To gain the most benefit from these boot camps, candidates should initially focus on self-study materials using the skill matrix, self-preparation books, and resources discussed previously, as well as master each individual technology from the blueprint. Only once they feel that they have achieved that peak level should candidates expect to gain maximum mileage from attending a boot camp.

Reference Books

No single resource for CCIE preparation is 100 percent comprehensive. You will likely need to review multiple books to prepare for CCIE Security certification and to master the different topics that are in the blueprints. Numerous books are available from Cisco Press and other third-party publishers. A list of recommended books to prepare for CCIE Security can be found at http://www.cisco.com/web/learning/le3/ccie/security/book_list.html.

Here are some recommended titles:

- *Network Security Technologies and Solutions*
- *CCIE Security Practice Labs (CCIE Self-Study)*
- *CCSP IPS Exam Certification Guide*
- *Cisco Access Control Security: AAA Administration Services*
- *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance*
- *Cisco ASA and PIX Firewall Handbook*
- *Cisco Network Security Troubleshooting Handbook*
- *Designing Network Security, Second Edition*
- *The Complete Cisco VPN Configuration Guide*
- *Troubleshooting Virtual Private Networks (VPN)*
- *Troubleshooting IP Routing Protocols*
- *Router Security Strategies: Securing IP Network Traffic Planes*

Here also is a compilation of additional supplementary online resources. Please use them to your advantage during self-study:
http://www.cisco.com/web/learning/le3/ccie/security/online_resources.html

Cisco Website CCO

Many candidates overlook one of the best resources for useful material and technical information that is also free to use—the Cisco website. A plethora of sample configurations and technical tips is available on support pages for each Cisco product and technology. These articles and whitepapers are written to reflect current trends and demands and include sample diagrams, configurations, and invaluable **show** and **debug** command outputs.

Cisco Learning Network

You can also use one of the most sought-after social learning network tools—Cisco Learning Network (CLN)—to enhance and advance your knowledge and to use it as the primary source for information sharing and learning. Browse the abundant technical content that is available there and share insights, opinions, and knowledge with the community. Visit the CLN portal at http://www.cisco.com/go/learnnetspace.

Community Forums

Additionally, technical forums can play an essential role for a candidate during exam preparation. You can generally find qualified CCIEs and other security engineers available 24 hours a day to help answer your queries and work through your technical problems. Group forums can play the escalation role during your preparation time by providing instantaneous technical support.

Here are some forums that might be of assistance:

- Cisco Networking Professional Connection (NetPro)
  http://www.cisco.com/go/netpro
  Candidates can post questions for technical assistance, seek suggestions, or share experiences at NetPro.

- Cisco Certification Community
  http://www.cisco.com/go/certcommunity
  Offers online resource for anyone who holds at least one Cisco certification. Community hosts numerous discussion groups for certified individuals.
- Cisco Certification Online Support
  http://www.cisco.com/go/certsupport
  Q&A on certification-related topics such as exam information, books, trainings, requirements, resources, tools, utilities and much more.

Cisco Technical Documentation Website

During the CCIE lab exam, there is only one resource available to assist you if you reach an impasse or need help—the Cisco Technical Documentation Website. You need to be able to navigate the Cisco documentation website with fluency and confidence. This resource is the only one that you are allowed to use during the exam, and you will need to be able to quickly look up anything that you need. Candidates should make navigating the Cisco documentation website part of their regular practice. If you are familiar with this integral resource, it can save you time during the exam.

Equipment for Studying (Home Lab vs. Rental Racks)

Arranging equipment for studying is by far one of the most important aspects for every CCIE candidate. Although acquiring a personal home lab is an ideal scenario, it can be costly to gather all of the equipment necessary to build a CCIE Security rack. However, you can start with just a few devices—three to four routers, a switch, and a Cisco ASA firewall. The goal should be to obtain a thorough understanding of the technologies and the architecture and also to know how they integrate with each other. For other hardware devices that are more costly and difficult to obtain, such as the Cisco IPS Sensor appliance and the Cisco VPN3000 Series Concentrator, it is recommended that you consider renting the equipment online.

If you are unable to establish your own home lab, an alternative is to rent a rack. Today, with high-speed broadband, it is very easy to obtain good Internet bandwidth and IP connectivity to remote sites. Rack rental is a remote service, where equipment is hosted on a remote location, and you can access it from your own home or place of work at your convenience. You generally need to schedule time slots to practice on remote equipment. There are many third-party vendors who provide rack rental services. This method is far less expensive than purchasing a home security rack.

Practice Labs

During your study, it is strongly recommended that you start with individual technologies and master each topic from the blueprint independently. When studying individual technologies such as firewalls, IPsec, AAA, and others, you might find that you can easily gain proficiency using them as standalone technologies. But integrating multiple technologies can be tricky and difficult at first. Your goal should be to become fluent in each topic on its own without having to worry about integrated technologies.

Later on, once you are confident in each topic, you should focus on multilayer, multifaceted, integrated technology practice labs and complex scenarios involving all of the topics from the blueprint. Find practice labs with complex scenarios that require you to integrate multiple technologies. By practicing with more complex lab exercises, you can improve your exam strategy and identify areas that require extra study. This approach will help you refocus and revise your study plan and adjust it accordingly.

In addition to technical skill, candidates must also focus on time management and exam-taking strategy, as they play a pivotal role to exam success. Practice labs not only help you asses your technical skills but also help you improve your time management and test-taking approach skills.

Troubleshooting

As many candidates might be aware, recent CCIE lab exams heavily focus on evaluation troubleshooting skills. Earlier exams were purely configuration-based, whereas newer exams have some troubleshooting-related questions.

There are currently two types of troubleshooting questions in the CCIE Security lab exam:

1. *Dedicated, explicitly marked troubleshooting questions*: These questions are clearly marked, and the exam identifies troubleshooting scenarios and explains that they are preconfigured with some broken configurations. Candidates need to identify the purposely injected faults and ensure functionality of the items.
2. *Integrated, embedded troubleshooting questions*: These questions are not marked as troubleshooting questions but are instead integrated into the topology. Troubleshooting is woven into the scenarios, and candidates may have to think over and beyond in order to achieve the task and ensure functionality. For example, there could be an IPsec LAN-to-LAN configuration, in which the candidate configures everything correctly; however, functionality is broken, and IPsec is not encrypting the required traffic. The problem could be embedded into the scenarios in such a way that you may need to open necessary ACL or address translation on the Cisco ASA firewall. Or perhaps an ACL on a device that sits between the IPsec peers is denying all ESP traffic (related to some other question), and so on.

When studying, it is recommended that candidates learn how to read debugs. For instance, you might begin by configuring a task such as IPsec LAN-to-LAN on a Cisco IOS router and turn on debugs. Then capture good **debugs** and copy them into your Notepad. Next, break your own work by misconfiguring something, for example, preshared keys, the wrong ACL, and so on. Finally, recapture bad **debugs** and compare them with the good **debugs**. This method is one of the best ways to learn the protocol in-depth and understand how it works.

Know how to troubleshoot extensively using the **show** and **debug** command outputs. Check for typos when configuring items, as this area presents some of the most common mistakes observed during exam grading. Keep in mind the point values; do not lose too much time working on a two- or three-point question. Verify functionality for each question before moving on. Remember, lack of functionality earns zero points.

Lab Exam Tips and Techniques

Finally, here is a list of “lab exam tips and techniques” that were compiled through day-to-day proctoring experience and watching what some candidates do best. Some of these items may seem trivial, but candidates tend to forget them:

- Read the entire exam first.
- Redraw topology (consolidate information from all of the diagrams given).
- Plan your exam using the “divide-and-conquer rule,” meaning plan your exam in segments. For example, you might group tasks into categories such as initializing firewall, initializing IPS, Layer 2 mappings, IP routing reachability, IP connectivity, and so on.
- Manage your time by the total number of sections questions.
- Make no assumptions.
- Ask the proctor for clarifications when needed.
- Observe the “10-minute rule,” meaning report any technical problems or hardware equipment issues to the proctor after troubleshooting on it for 10 minutes (and only if you are convinced that your configuration is absolutely correct).
- Keep a list of everything in order to revisit, recheck, or reverify items before the end of the exam.
- Work questions as a unit.
- Some questions are independent, and some are interdependent. Read carefully.
- Test your work; functionality is important. Do not rely on configuration only.

- Frequently save configurations.
- Minimize last-minute changes.
- Plan for at least 30-45 minutes towards the exam end to reverify all of your work from the beginning.
- Reduce stress by arriving early at the exam location.
- Leave yourself time—the exam can run over due to unforeseen circumstances, such as power issues, faulty hardware, fire drills, and so on.

Final Word

It is hoped that the preceding tips and information will help you succeed in achieving the CCIE Security certification. Passing the CCIE exam is a great source of satisfaction and can boost your career to the next level. The secret to success on CCIE, as with most endeavors, is motivation, dedication, and consistency. In the long run, being an expert in the field of security networking is not just a destination, but an ongoing journey. You are wished all the best in the pursuit of excellence.

For more information about CCIE programs, visit the CCIE website at http://www.cisco.com/go/ccie.

