Cisco Security Certifications

Overview

Increasing Demand for Practical Network Security Skills
Cisco has taken note of the evolution of the role of the network security professional and its relevance to the industry. The speed at which network security is evolving demands more practical, hands-on skills in network security engineering and has made network security performance more visible to the entire organization. Network security engineers in the marketplace today understand the products and the discipline of good network security, the practices and compliance mandates of industry and government, and the need to protect their organizations from increasingly sophisticated threats to their systems. Cisco network security engineers have real-world security implementation and troubleshooting skills.

Job-Ready Practical Skills
The Cisco CCNA® Security, CCNP® Security, and CCIE® Security certification programs are practical, relevant, and job-ready certification curricula aligned closely with the specific tasks expected of these in-demand professionals. Cisco realizes that the network security professional increasingly must focus on design, configuration, and support responsibilities as the technical consultant and device specialist or expert on a security team. Therefore, the Cisco Security curriculum is specific to the best practices of network security administrators, engineers, and experts using the latest Cisco equipment, devices, and appliances.

Network Security Best Practices
The CCNA Security, CCNP Security, and CCIE Security programs validate basic through advanced knowledge of the skills required to design, configure, and engineer secure network infrastructures using the latest Cisco security devices, technologies, and appliances. The curricula emphasize the real-world best practices of network security using the features of Cisco IOS® Software security, Cisco ASA adaptive security appliance secure virtual private networks (VPNs), Cisco Intrusion Prevention System (IPS), and Cisco security management tools and using the techniques to optimize these technologies in a single, integrated network security solution.

Achieving CCNA Security Certification

CCNA Security certification offers professionals job-ready training and skills. The certification lays the foundation for job roles such as network security specialist, security administrator, and network security support engineer. Candidates gain knowhow in securing Cisco routers and switches and their associated networks.

Requirements
The CCNA Security program is a three-year certification program intended to provide baseline security education and testing for network professionals interested in network security. Relevant skills learned include testing, deploying, configuring, maintaining, and troubleshooting Cisco network security appliances and Cisco IOS Software devices that establish the security posture of the network. Before attempting the CCNA Security certification, candidates must meet the

requirements for Cisco CCNA certification and have at least one to three years of experience in the field of networking.

Prerequisite Skills and Knowledge
Completion of the CCNA certification requires the prerequisite exams and recommended training shown in Table 1.

Table 1 CCNA Security

Required Exams	Exam Name and Recommended Training
640-802 or 640-822 and 640-816	CCNA Composite or Interconnecting Cisco Network Devices 1 (ICND1) and Interconnecting Cisco Network Devices 2 (ICND2)

Completion of the CCNA Security curriculum requires the exam and recommended training shown in Table 2.

Table 2 CCNA Security

Required Exam	Exam Name and Recommended Training
640-553	Implementing Cisco IOS Network Security (IINS)

CNSS 4011 Recognition
The U.S. National Security Agency (NSA) and the Committee on National Security Systems (CNSS) recognize that Cisco CCNA Security courses meet the CNSS 4011 training standard. Compliance with this standard means that the Cisco CCNA Security certification program provides the required training for network security professionals who assist federal agencies and private sector entities to protect their information and aid in the defense of information resources vital to the nation.

This standard is intended for information security professionals responsible for identifying system vulnerabilities, investigating and documenting system security technologies and policies, and analyzing and evaluating system security technologies.

Achieving CCNP Security Certification

In the demanding security environment, CCNP Security certification offers employers proof of job-ready training and skills from experienced, professional-level network security engineers. Industry forecasts show that, in the next five years, the number of network security professionals will need to double, and most of these professionals will need the validation of an industry certification.

Requirements
The CCNP Security program is a three-year certification program intended to distinguish the Cisco network security engineers who have the necessary skills to test, deploy, configure, maintain, and troubleshoot the Cisco network security appliances and Cisco IOS Software devices that establish the security posture of the network. Before attempting the CCNP Security certification or any of its associated security specialist certifications, individuals must meet the requirements for the Cisco CCNA Security certification and have at least one to three years of experience in the field of network security.

Prerequisite Skills and Knowledge
Completion of the CCNA Security certification requires the prerequisite exams and recommended training that was shown in Table 1.

The CCNP Security curriculum requires the exams and recommended training shown in Table 3.

Table 3 CCNP Security

Required Exams	Exam Name and Recommended Training
642-637	Securing Networks with Cisco Routers and Switches (SECURE)
642-627	Implementing Cisco Intrusion Prevention System (IPS)
642-617	Deploying Cisco ASA Firewall Solutions (FIREWALL)
642-647	Deploying Cisco ASA VPN Solutions (VPN)

CISCO

CNSS 4013 Recognition

The U.S. National Security Agency (NSA) and the Committee on National Security Systems (CNSS) recognize that Cisco security courseware meets the CNSS 4013 training standard. This compliance means that the Cisco CCNP Security certification program provides the required training for network security professionals who assist federal agencies and private sector entities to protect their information and aid in the defense of information resources vital to the nation.

This advanced standard is intended for system administrators responsible for the security oversight or management of critical networks.

The formal NSA and CNSS certification gives Cisco the authority to recognize candidates who have demonstrated that they have met the CNSS 4013 training standard. Candidates who have met the standard are issued a letter of recognition acknowledging their completion of the related requirements. This letter of recognition can be used as confirmation of having met the CNSS 4013 requirements.

Achieving CCIE Security Certification

The CCIE Security Program recognizes individuals who have the knowledge and skills to implement, maintain, and support extensive Cisco network security solutions using the latest industry best practices and technologies. This program is the industry standard for recognition and rewards for network security engineers who have demonstrated expert-level performance in implementation, configuration, and troubleshooting of Cisco network security solutions.

Requirements

The CCIE Security program is a two-year certification program intended to recognize the Cisco network security experts who have the necessary skills to test, deploy, configure, maintain, and troubleshoot Cisco network security appliances and Cisco IOS Software devices that establish the security posture of the network. Attaining and maintaining this performance-based, practical certification proves skills that are only achievable by distinct experts in the network security field. This certification carries prestige that is envied by security professionals worldwide. To gain Security CCIE certification, candidates not only must prove their theoretical knowledge of security best practices but also must demonstrate them in a lab environment with real equipment using real-world scenarios.

Prerequisite Skills and Knowledge

There are no formal prerequisites for Cisco CCIE certification. Candidates must first pass a written qualification exam and then pass the corresponding hands-on lab exam. Candidates are expected to have an in-depth understanding of the exam topics and are strongly encouraged to have three to five years of job experience before attempting certification.

The CCIE Security curriculum requires the exams shown in Table 4.

Table 4 CCIE Security

Required Exams	Exam Name
350-018	CCIE Security Written Exam
CCIE Security Lab Exam v4.0	CCIE Security Lab Exam v4.0

CCNP Security Product and Technology Security Specialist

Within the CCNP Security curriculum are several network security engineering specialist certifications for cross-training and staff development. Intended for individuals who specialize in one or more technologies or products that make up the network security infrastructure, these specialist certifications offer a convenient validation of skills and competency in intrusion prevention, VPNs, perimeter firewalls, high availability, IEEE 802.1x, mobile access, Network Admission Control (NAC), and the Cisco IOS Software security features embedded in the latest Cisco routers and switches.

The following security specialist certifications are included in the CCNP Security curriculum.

Cisco ASA Security Specialist

The Cisco ASA Security Specialist certification recognizes security professionals who have attained specialized, in-depth expertise in the recommended best practices for designing, implementing, maintaining, and troubleshooting network security solutions using the adaptive security appliance technologies. The Cisco ASA adaptive security appliance is a best-in-class product, widely deployed and in use at leading enterprises and service providers worldwide. The

Cisco ASA Security Specialist certification is recognized as the benchmark security product certification for engineers, consultants, and architects who configure advanced Cisco ASA adaptive security appliance firewalls and VPN solutions, including advanced protocol handling, remote-access VPNs, Cisco IOS SSL VPNs, site-to-site VPNs, high-availability VPNs, and failover features (see Table 5).

Table 5 Cisco ASA Security Specialist Certification

Required Exams	Exam Name and Recommended Training
642–617	Deploying Cisco ASA Firewall Solutions (FIREWALL)
642–647	Deploying Cisco ASA VPN Solutions (VPN)

Cisco Firewall Security Specialist

Cisco firewalls are ubiquitous in the world of network security today. Professionals with the skills to design, implement, and maintain Cisco firewall solutions using the Cisco ASA adaptive security appliance and zone-based firewall solutions in Cisco routers and switches are in high demand. The Cisco Firewall Security Specialist certification focuses on validating the skills and knowledge needed to implement perimeter security solutions using Cisco security appliances. These certified specialists are actively involved in developing secure business solutions and designing and delivering multiple levels of secure access to the network (see Table 6).

Table 6 Cisco Firewall Security Specialist Certification

Required Exams	Exam Name and Recommended Training
642–617	Deploying Cisco ASA Firewall Solutions (FIREWALL)
642–637	Securing Networks with Cisco Routers and Switches (SECURE)

Cisco IOS Security Specialist

The Cisco IOS Software security specialist demonstrates the hands-on knowledge and skills that are required to secure networks using Cisco IOS Software security features embedded in the latest Cisco routers and switches and the widely deployed Cisco security appliances. Cisco IOS Software security specialists are able to secure the network environment and provide security services based on Cisco IOS Software: zone-based policy firewall; Cisco IOS Software IPS; user-based firewall; secure tunnels using IP Security (IPsec) VPN technology, including public key infrastructure (PKI), virtual tunnel interface (VTI) and dynamic VTI (DVTI), Group Encrypted Transport VPN (GET VPN), and Dynamic Multipoint VPN (DMVPN); 802.1x authentication; and advanced switch security features (see Table 7).

Table 7 Cisco IOS Security Specialist Certification

Required Exam	Exam Name and Recommended Training
642–637	Securing Networks with Cisco Routers and Switches (SECURE)

Cisco IPS Security Specialist

The Cisco IPS appliance is a primary device to maintain the security posture of networks. Information systems security (infosec) and network professionals who have the skills to properly deploy and configure the Cisco IPS appliance are in high demand. Cisco IPS specialists are professionals who can deploy, configure, and troubleshoot this appliance to work effectively in a complete security solution. Cisco IPS specialists can operate and monitor Cisco IOS Software and IPS technologies to prevent, understand, and respond to intrusion attempts (see Table 8).

Table 8 Cisco IPS Security Specialist Certification Required

Required Exam	Exam Name and Recommended Training
642–627	Implementing Cisco Intrusion Prevention System (IPS)

CISCO

Cisco VPN Security Specialist

Cisco offers numerous VPN solutions and configurations. Cisco VPN solutions are widely deployed in many networks today. Enterprises and service providers deploy numerous VPN solutions at any given time for their various customers and organizations, from simple point-to-point tunneling to multilayer, dynamic, high-availability VPNs. Cisco VPN security specialists can configure, maintain, and troubleshoot these VPN solutions using Cisco IOS Software and the robust Cisco ASA adaptive security appliance (see Table 9).

Table 9 Cisco VPN Security Specialist Certification

Required Exams	Exam Name and Recommended Training
642-637	Securing Networks with Cisco Routers and Switches (SECURE)
642-647	Deploying Cisco ASA VPN Solutions (VPN)

Recertification

Cisco CCNP Security exams can be used to recertify your associate, professional and security specialist certifications. Achieving or recertifying any of the certifications that are detailed in Tables 3 through 9 automatically extends active associate, specialist, and professional-level certifications up to the point of expiration of the last certification achieved. Cisco professional-level certifications are valid for three years, and specialist certifications are active for two years. To recertify, certificate holders should pass any 642 exam that is part of the professional-level curriculum, or any Cisco CCIE written exam, or Cisco CCDE® written exam, or current CCDE practical exam, or CCAR® interview and the CCAR board review before the certification expiration date.

Learn More

For more information or to register for this program, visit www.ciscolearningnetwork.com.