



CCIE SECURITY V6.1

CCIE Security Certification v6.1 is the highest and most prestigious certification from Cisco. It ranks No.1 in the 10 Most Difficult IT Certifications list and is highly valued worldwide. A CCIE certified individual is an elite title in the field of network and security engineering, proving their mastery in their domain of Cisco security. The CCIE Security Certified experts have the knowledge and skills required to architect, engineer, implement, troubleshoot, and support the full suite of Cisco security technologies, using the latest methods to protect systems and environments against every kind of modern security risks, threats, and vulnerabilities. The CCIE SecurityV6.1 program is designed to include direct exposure on real Cisco Routers, Switches, Cisco ASA Firewalls, FTD(Firepower), ISE,WSA Iron port and Cisco NGIPS, Umbrella, Stelthwatch ,DNAC,ESA and FireAMP.

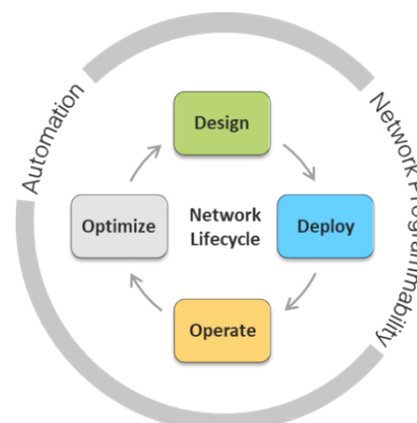


The quality of the program, the testing methods, and the relevance of this certification enhances its value. At IPRulers, the classes are facilitated by CCIE Security certified and experienced instructors, and students will be exposed to the latest equipment's. With grouped as well as one-to-one classes and online tutorials that could be scheduled for weekdays or weekends in accordance to the students' choice, IPRulers is fast becoming a leading name in Dubai, UAE in achieving high-value Cisco Certification with a significant pass rate on the first attempt.

COURSE DETAILS

CCIE Security v6.1 certification is the avatar of core knowledge and practical skills in the management of the most complex scenarios of the entire IT Security of a network lifecycle (Designing, Deploying, Operating & Optimizing). IPRulers provide CCIE Security v6.1 training. just as per the course described by the Cisco Security Certification blueprint.

The new method adapted for CCIE Exam is given below, which have vital parts known as DESIGN, DEPLOY, OPERATE & OPTIMIZE.



THE CCIE SECURITY V6.1 CERTIFICATION IS ACHIEVED WITH TWO EXAMS.



Step 1: Pass the qualifying exam

IMPLEMENTING AND OPERATING CISCO SECURITY CORE TECHNOLOGIES (350-701 SCOR V1.1)

The 120-minute, the qualifying exam, Implementing and Operating Cisco Security Core Technologies exam is associated with the CCNP Security, Cisco Certified Specialist (with core subject Security CORE), and CCIE security Certifications. It tests a candidate's knowledge of security infrastructure Firewalls, NGIPS, Cisco ISE, Web Security, Email security, and VPN. Clearing this exam gives a Specialist Certification, to recognize all accomplishments of the candidate.

Step 2: Pass the lab exam

CCIE SECURITY V6.1 LAB EXAM

The Cisco CCIE Security Network Security Lab Exam is an eight-hour, hands-on lab exam that requires a candidate to do the end-to-end lifecycle of complex security solutions and technologies, from designing and deploying to operating and optimizing. The Cisco CCIE Security Network Security Lab that requires a candidate to plan, design, deploy, operate, and optimize dual stack solutions (IPv4 and IPv6) for complex enterprise networks.

	Module 1	Module 2
	Design	Deploy, Operate, Optimize
Time	3 hours (fixed)	5 hours (fixed)
Format	Scenario based	Hands-on + Web- based items
Backward Navigation within the module	Disabled	Enabled
Point Values	Hidden	Shown

PREREQUISITES

The CCIE Security V6.1 does not require any qualification for attendance of the course. However, comprehensive knowledge of the subjects is necessary for attending the examinations.

Five to seven years' experience in networking field, especially in designing, deploying, operating and optimizing security technologies will be an advantage to attempt the CCIE examination.

COURSE OUTLINE

1.0 Perimeter Security and Intrusion Prevention (20%)

1.1 Deployment modes on Cisco ASA & Cisco FTD

- 1.1.a Routed
- 1.1.b Transparent
- 1.1.c Single
- 1.1.d Multi-context
- 1.1.e Multi-instance

1.2 Firewall features on Cisco ASA & FTD

- 1.2.a NAT
- 1.2.b Application inspection
- 1.2.c Traffic zones
- 1.2.d Policy-based routing
- 1.2.e Traffic redirection to service modules
- 1.2.f Identity firewall

1.3 Security features on Cisco IOS/IOS XE

- 1.3.a Application awareness
- 1.3.b Zone-based firewall
- 1.3.c NAT

1.4 Cisco FMC features

- 1.4.a Alerting
- 1.4.b Logging
- 1.4.c Reporting
- 1.4.d Dynamic objects

1.5 Cisco NGIPS deployment modes

- 1.5.a In-line
- 1.5.b passive
- 1.5.c TAP

1.6 Cisco NGFW features

- 1.6.a SSL inspection
- 1.6.b User identity
- 1.6.c Geolocation
- 1.6.d AVC

1.7 Detect and mitigate common types of attacks

- 1.7.a DoS/DDoS
- 1.7.b Evasion techniques
- 1.7.c Spoofing
- 1.7.d Man-in-the-middle
- 1.7.e Botnet

1.8 Clustering and high availability features on Cisco ASA and Cisco FTD

1.9 Policies and rules for traffic control on Cisco ASA and Cisco FTD

1.10 Routing protocols security on Cisco IOS, Cisco ASA, and Cisco FTD

1.11 Network connectivity through Cisco ASA and Cisco FTD

1.12 Correlation and remediation rules on Cisco FMC

2.0 Secure Connectivity and Segmentation (20%)

2.1 Cisco AnyConnect client-based, remote-access VPN technologies on Cisco ASA, Cisco FTD, and Cisco routers

2.2 Cisco IOS CA for VPN authentication

2.3 FlexVPN, DMVPN, and IPsec L2L tunnels

2.4 VPN high availability methods

- 2.4.a Cisco ASA VPN clustering
- 2.4.b Dual-hub DMVPN deployments

2.5 Infrastructure segmentation methods

- 2.5.a VLAN
- 2.5.b PVLAN
- 2.5.c GRE
- 2.5.d VRF-Lite
- 2.6 Microsegmentation with Cisco TrustSec using SFT and SXP

3.1 Device hardening techniques & control plane protection methods

- 3.1.a CoPP
- 3.1.b IP source routing
- 3.1.c iACLs

3.2 Management plane protection techniques

- 3.2.a CPU
- 3.2.b Memory thresholding
- 3.2.c Securing device access

3.3 Data plane protection techniques

- 3.3.a uRPF
- 3.3.b QoS
- 3.3.c RTBH

3.4 Layer 2 security techniques

- 3.4.a DAI
- 3.4.b IPDT
- 3.4.c STP security
- 3.4.d Port security
- 3.4.e DHCP snooping
- 3.4.f RA Guard
- 3.4.g VACL

3.5 Wireless security technologies

- 3.5.a WPA
- 3.5.b WPA2
- 3.5.c WPA3
- 3.5.d TKIP
- 3.5.e AES

3.6 Monitoring protocols

- 3.6.a NetFlow/IPFIX/NSEL
- 3.6.b SNMP
- 3.6.c SYSLOG
- 3.6.d RMON
- 3.6.e eStreamer

3.7 Security features to comply with organizational security policies, procedures, and standards BCP 38

- 3.7.a ISO 27001
- 3.7.b RFC 2827
- 3.7.c PCI-DSS

3.8 Cisco SAFE model to validate network security design and to identify threats to different PINs

3.9 Interaction with network devices through APIs using basic Python scripts

- 3.9.a REST API requests and responses
- 3.9.b Data encoding formats

3.10 Cisco DNAC Northbound APIs use cases

- 3.10.a Authentication and authorization
- 3.10.b Network discovery
- 3.10.c Network device
- 3.10.d Network host

4.0 Identity Management, Information Exchange, & Access Control (25%)



- 4.1 Cisco ISE scalability using multiple nodes and personas
- 4.2 Cisco switches and Cisco Wireless LAN Controllers for network access AAA with Cisco ISE
- 4.3 Cisco devices for administrative access with Cisco ISE
- 4.4 AAA for network access with 802.1X and MAB using Cisco ISE
- 4.5 Guest lifecycle management using Cisco ISE and Cisco WLC
- 4.6 BYOD on-boarding and network access flows
- 4.7 Cisco ISE integration with external identity sources
 - 4.7.a LDAP
 - 4.7.b AD
 - 4.7.c External RADIUS
- 4.8 Provisioning Cisco AnyConnect with Cisco ISE and Cisco ASA
- 4.9 Posture assessment with Cisco ISE
- 4.10 Endpoint profiling using Cisco ISE and Cisco network infrastructure including device sensor
- 4.11 Integration of MDM with Cisco ISE
- 4.12 Certification-based authentication using Cisco ISE
- 4.13 Authentication methods
 - 4.13.a EAP Chaining and TEAP
 - 4.13.b MAR
- 4.14 Identity mapping on Cisco ASA, Cisco ISE, Cisco WSA, and Cisco FTD
- 4.15 pxGrid integration between security devices Cisco WSA, Cisco ISE, and Cisco FMC
- 4.16 Integration of Cisco ISE with multifactor authentication
- 4.17 Access control and single sign-on using Cisco DUO security technology
- 4.18 Cisco IBNS 2.0 (C3PL) for authentication, access control, and user policy enforcement

5.0 Advanced Threat Protection & Content Security (20%)

- 5.1 Cisco AMP for networks, Cisco AMP for endpoints, and Cisco AMP for content security (Cisco ESA, and Cisco WSA)
- 5.2 Detect, analyze, and mitigate malware incidents
- 5.3 Perform packet capture and analysis using Wireshark, tcpdump, SPAN, ERSPAN, and RSPAN
- 5.4 Cloud security
 - 5.4.a DNS proxy through Cisco Umbrella virtual appliance
 - 5.4.b DNS security policies in Cisco Umbrella
 - 5.4.c RBI policies in Cisco Umbrella
 - 5.4.d CASB policies in Cisco Umbrella
 - 5.4.e DLP policies in Cisco Umbrella

5.5 Web filtering, user identification, and Application Visibility and Control (AVC) on Cisco FTD and Cisco WSA

5.6 WCCP redirection on Cisco devices

5.7 Email security features

5.7.a Mail policies

5.7.b DLP

5.7.c Quarantine

5.7.d Authentication

5.7.e Encryption

5.8 HTTP decryption and inspection on Cisco FTD, Cisco WSA, and Cisco Umbrella

5.9 Cisco SMA for centralized content security management

5.10 Cisco advanced threat solutions and their integration:

Cisco Stealthwatch, Cisco FMC, Cisco AMP, Cisco CTA, Threat Grid, ETA, Cisco WSA, Cisco SMA, Cisco Threat Response, and Cisco Umbrella

CCIE SECURITY V6.1: EQUIPMENT AND SOFTWARE LIST

The practical exam tests candidates on solutions that can be configured using the equipment and software versions below. Candidates may see more recent software versions during their attempt, but they will be tested only on features in this list.

Passing the exam requires a depth of understanding that is difficult to obtain without hands-on experience. Early in your preparation, you should arrange access to equipment and software like that used on the exam.

Virtual Machines

- ▶ Cisco Identity Services Engine (ISE): 3.1.0
- ▶ Cisco Web Security Appliance (WSA): 9.2
- ▶ Cisco Email Security Appliance (ESA): 11.1
- ▶ Cisco Firepower Management Center Virtual Appliance: 7.1
- ▶ Cisco Firepower NGIPSv: 7.0
- ▶ Cisco Firepower Threat Defense: 6.2
- ▶ Cisco Adaptive Security Virtual Appliance (ASAv): 9.4(3)
- ▶ Cisco CSR 1000V Series Cloud Services Router: 15.5.(3), 16.6.3
- ▶ Cisco Stealthwatch SMC-FC: 6.10
- ▶ Cisco FireAMP Cloud: 5.3
- ▶ Cisco Wireless Controller (WLC): 8.3
- ▶ Cisco DNA Center Release 2.2.2.4
- ▶ L2IOSv: 15.2

Physical Equipment

- ▶ Cisco Adaptive Security Appliance: ASA5512: 9.2
- ▶ Cisco Adaptive Security Appliance: ASA5516: 9.8
- ▶ Cisco Catalyst Switch: C3650: 16.6
- ▶ Cisco Catalyst Switch: C3850: 3.7
- ▶ Cisco Wireless Access Point: AP1852: 8.3

Cloud-delivered

- ▶ Cisco Umbrella

Other

- ▶ Test PC: Windows 10 Enterprise
- ▶ AD/DNS: Window Server 2016
- ▶ Linux Kali: 4.17
- ▶ Cisco AnyConnect: 4.2



Classroom-based Training	Online Training	Corporate Training
<p>Go old-school. Make friends and have fun, just like elementary grades. Follow lectures, turn in assignments and appear for exams in campus-style!</p>	<p>Sit in the comfort of your home as you move through the course. Instructors will guide you in predetermined sessions. Hundreds of supporting videos available, in case you want to outshine yourself.</p>	<p>Lectures and hands-on training for office employees, in the comfort of their own office. Sponsored by employers to push up their employees above the market competence.</p>
One-on-One Training	Fast Track Training	Private Group Training
<p>An instructor will train you in private – without any external intrusion. Ideal if you want to progress on your own. Schedule your classes according to your own timeline as you advance, without disruption to your daily routine.</p>	<p>No time to follow regular class timeline? Go fast track – speed through the course, whether it be alone, or online, in groups, on an accelerated timescale, to give the icing on the cake.</p>	<p>You and your friends like to be together in a class, but without any outsiders? You've got it! Feel as if you have hired your own instructor. A way to combat shyness, with the comfort your friend-circle.</p>
Lab workshop training		
<p>This would be helpful for those who are already familiar with the technologies in depth with hands-on to clear their ccie lab exam.</p>		

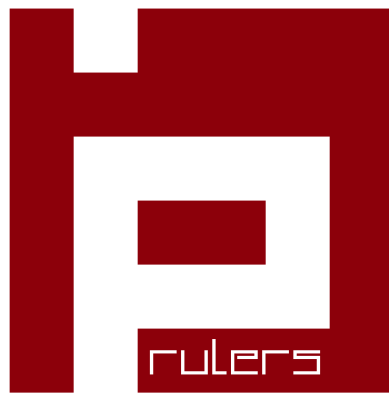
- ▶ Network engineers attempting the core exam – Implementing and Operating Cisco Enterprise Network Core Technologies (SCOR 350- 701 V1.1).
- ▶ Network engineers who have five to seven years of professional experience in designing, deploying, operating, and optimizing enterprise networking technologies.
- ▶ Network designers who design and support complex network technologies and topologies.
- ▶ Network engineers who use an expert-level problem-solving process (including options analysis) to support complex network technologies and topologies
- ▶ IT students and professionals seeking strong expertise in the subject and an internationally recognized qualification in the same for prospective jobs.
- ▶ Candidates with CCNP Enterprise Certification, moving on to expert levels.


TRAINER'S PROFILE

- ▶ IP Rulers is managed by an expert team of trainers with over 15 years' experience in the industry and in hands-on training.
- ▶ All the trainers have multiple CCIEs in their respective areas of interest.
- ▶ Individual trainers' profiles can be provided upon request by email, along with demos and LinkedIn profiles.
- ▶ Online and classroom demos are also available upon request

BENEFITS

- ▶ Job roles of elite executives in the fast-paced world of Enterprise network.
- ▶ Industry-level knowledge and direct experience in implementation of core Cisco enterprise infrastructure solutions.
- ▶ Ability to recognize customer requirements and support proposed solutions.
- ▶ Enhanced job opportunities with sky-high career growth, coupled with respectable compensations.
- ▶ Expertise in all stages of implementing complex networking solutions – from creation and analysis, to operation and optimization.
- ▶ Essential skills in networking automation and network programmability in the fast-changing world of technology.
- ▶ Specialist Certification for clearing the qualifying exam.
- ▶ Authority to link the CCIE Certification Badge to all social media profiles.



 IP Rulers, 201, Wasl Business Central. 29B street, Sheikh Rashid Road. Port Saeed, Dubai.

 www.iprulers.com

 training@iprulers.com

 +971559454771 | +97143346660