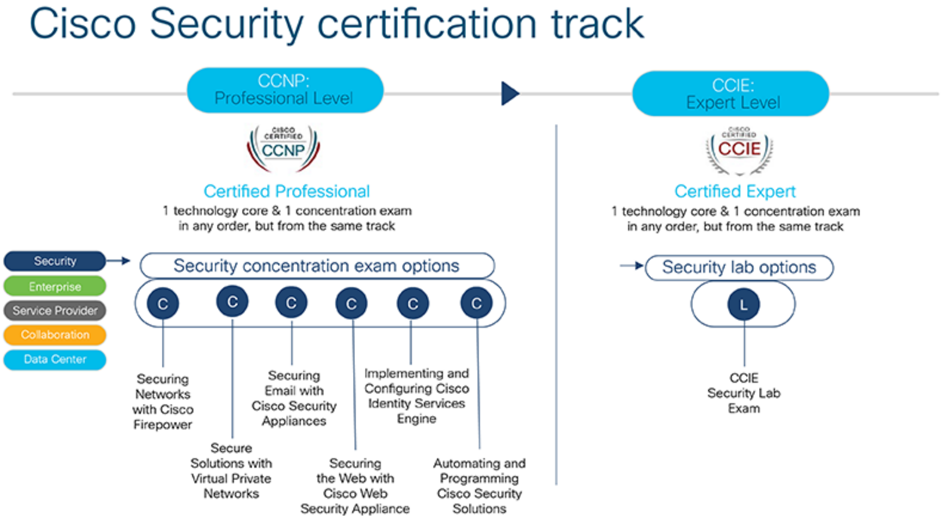
CCNP SECURITY

www.iprulers.com training@iprulers.com

IP Rulers is the new face of **CCNP Security Certification and Training** in Dubai, UAE, which provides both online and classroom-based training in the latest cutting-edge technologies in the IT infrastructure security and networking portfolio. With grouped as well as one-to-one classes and online tutorials that could be scheduled for week-days or weekends in accordance to the students' choice, IP Rulers is fast becoming a leading name in Dubai in providing a highly valued Cisco Certificate with a 100% pass rate on the first attempt. The IP Rulers CCNP Security Certification Program is a testimony to a candidate's network security skills for security in routers, Switches, Firewalls, networking devices, and appliances. It provides in-depth technology classes inthe skills required to choose, deploy, support and troubleshoot ASA, FTD, VPNs, ISE, WSA, ESA and NGIPS solutions for their enterprise networking environments. With a CCNP Security certification obtained under an expert team of trainers who have multiple CCIEs with experience in the industry and hands-on training, candidates are geared up to face complex networks for core technologies, optimized infrastructure, secure applications and efficient performance.

COURSE DETAILS

The CCNP Security Certification comprises of clearing two exams – one in a core subject, and another in a concentration subject. This gives a CCNP Security Badge. Clearing only the core subject gives a Core Specialist Badge, which is also the qualification for CCIE Security Certification. This exam focuses on skills and technologies to provide Cisco security solutions against cyber security attacks. Achieving only the concentration subject gives a Concentration Specialist Badge. This exam focuses on new, distinct subjects related to job-specific roles.


Cisco Security certification track
CCNP:
Professional Level
CISCO CERTIFIED
CCNP
Certified Professional
1 technology core & 1 concentration exam
in any order, but from the same track
CCIE:
Expert Level
CISCO CERTIFIED
CCIE
Certified Expert
1 technology core & 1 concentration exam
in any order, but from the same track
Security
Enterprise
Service Provider
Collaboration
Data Center
Security concentration exam options
C
C
C
C
C
C
Securing Networks with Cisco Firepower
Secure Solutions with Virtual Private Networks
Securing Email with Cisco Security Appliances
Securing the Web with Cisco Web Security Appliance
Implementing and Configuring Cisco Identity Services Engine
Automating and Programming Cisco Security Solutions
Security lab options
L
CCIE Security Lab Exam

The CCNP Security certification is achieved with two exams

CCNP Security Core exam:

350-701 SCOR Implementing and Operating Cisco Security Core Technologies (SCOR)

Objectives

- Describe information security concepts and strategies within the network
- Describe common TCP/IP, network application, and endpoint attacks
- Describe how various network security technologies work together to guard against attacks
- Implement access control on Cisco ASA appliance and Cisco Firepower Next-Generation Firewall
- Describe and implement basic email content security features and functions provided by Cisco Email Security Appliance
- Describe and implement web content security features and functions provided by Cisco Web Security Appliance
- Describe Cisco Umbrella® security capabilities, deployment models, policy management, and Investigate console
- Introduce VPNs and describe cryptography solutions and algorithms
- Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco Firepower Next-Generation Firewall (NGFW)
- Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and Extensible Authentication Protocol (EAP) authentication

- Provide basic understanding of endpoint security and describe Advanced Malware Protection (AMP) for Endpoints architecture and basic features
- Examine various defenses on Cisco devices that protect the control and management plane
- Configure and verify Cisco IOS software Layer 2 and Layer 3 data plane controls
- Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions
- Describe basics of cloud computing and common cloud attacks and how to secure cloud environment.

Concentration exams (choose one):

300-710 SNCF **Securing Networks with Cisco Firepower Next Generation Firewall (SSNGFW)**

Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS)

Objectives

- Describe key concepts of NGIPS and NGFW technology and the Cisco Firepower Threat Defense system, and identify deployment scenarios
- Perform initial Cisco Firepower Threat Defense device configuration and setup tasks
- Describe how to manage traffic and implement Quality of Service (QoS) using Cisco Fire power Threat Defense
- Describe how to implement NAT by using Cisco Firepower Threat Defense
- Perform an initial network discovery, using Cisco Firepower to identify hosts, applications, and services
- Describe the behavior, usage, and implementation procedure for access control policies
- Describe the concepts and procedures for implementing security intelligence features
- Describe Cisco Advanced Malware Protection (AMP) for Networks and the procedures for implementing file control and advanced malware protection
- Implement and manage intrusion policies
- Describe the components and configuration of site-to-site VPN
- Describe and configure a remote-access SSL VPN that uses Cisco AnyConnect®
- Describe SSL decryption capabilities and usage
- Describe the components of Cisco Firepower Threat Defense and the managed device registration process
- Detail Next-Generation Firewalls (NGFW) traffic control and configure the Cisco Firepower system for network discovery
- Implement access control policies and describe access control policy advanced features

- Configure security intelligences features and the Advanced Malware Protection (AMP) for Networks implementation procedure for file control and advanced malware protection
- Implement and manage intrusion and network analysis policies for NGIPS inspection
- Describe and demonstrate the detailed analysis techniques and reporting features provided by the Cisco Firepower Management Center
- Integrate the Cisco Firepower Management Center with an external logging destination
- Describe and demonstrate the external alerting options available to Cisco Firepower Management Center and configure a correlation policy
- Describe key Cisco Firepower Management Center software update and user account management features
- Identify commonly misconfigured settings within the Cisco Firepower Management Center and use basic commands to troubleshoot a Cisco Firepower Threat Defense device

300-715 SISE Implementing and Configuring Cisco Identity Services Engine (SISE)

Objectives

- Describe Cisco ISE deployments, including core deployment components and how they interact to create a cohesive security architecture. Describe the advantages of such a deployment and how each Cisco ISE capability contributes to these advantages
- Describe concepts and configure components related to 802.1X and MAC Authentication Bypass (MAB) authentication, identity management, and certificate services
- Describe how Cisco ISE policy sets are used to implement authentication and authorization, and how to leverage this capability to meet the needs of your organization
- Describe third-party Network Access Devices (NADs), Cisco TrustSec®, and Easy Connect
- Describe and configure web authentication, processes, operation, and guest services, including guest access components and various guest access scenarios
- Describe and configure Cisco ISE profiling services, and understand how to monitor these services to enhance your situational awareness about network-connected endpoints. Describe best practices for deploying this profiler service in your specific environment
- Describe BYOD challenges, solutions, processes, and portals. Configure a BYOD solution, and describe the relationship between BYOD processes and their related configuration components. Describe and configure various certificates related to a BYOD solution
- Describe the value of the My Devices portal and how to configure this portal
- Describe endpoint compliance, compliance components, posture agents, posture deployment and licensing, and the posture service in Cisco ISE
- Describe and configure TACACS+ device administration using Cisco ISE, including command sets, profiles, and policy sets. Understand the role of TACACS+ within the Authentication, Authentication, and Accounting (AAA) framework and the differences between the RADIUS and TACACS+ protocols
- Migrate TACACS+ functionality from Cisco Secure Access Control System (ACS) to Cisco ISE, using a migration tool

300-720 SESA Securing Email with Cisco Email Security Appliance (SESA)

Objectives

- Describe and administer the Cisco Email Security Appliance (ESA)
- Control sender and recipient domains
- Control spam with Talos SenderBase and anti-spam
- Use anti-virus and outbreak filters
- Use mail policies
- Use content filters
- Use message filters to enforce email policies
- Prevent data loss
- Perform LDAP queries
- Authenticate Simple Mail Transfer Protocol (SMTP) sessions
- Authenticate email
- Encrypt email
- Use system quarantines and delivery methods
- Perform centralized management using clusters
- Test and troubleshoot

300-725 SWSA Securing the Web with Cisco Web Security Appliance (SWSA)

Objectives

- Describe Cisco WSA
- Deploy proxy services
- Utilize authentication
- Describe decryption policies to control HTTPS traffic
- Understand differentiated traffic access policies and identification profiles
- Enforce acceptable use control settings
- Defend against malware
- Describe data security and data loss prevention
- Perform administration and troubleshooting

300-725 SWSA Securing the Web with Cisco Web Security Appliance (SWSA)

Objectives

- Introducing VPN Technology Fundamentals
- Implementing Site-to-Site VPN Solutions
- Implementing Cisco Internetwork Operating System (Cisco IOS®) Site-to-Site FlexVPN Solu tions
- Implement Cisco IOS Group Encrypted Transport (GET) VPN Solutions
- Implementing Cisco AnyConnect VPNs
- Implementing Clientless VPNs

Objectives

- Introducing Cisco Security APIs
- Consuming Cisco Advanced Malware Protection APIs
- Using Cisco ISE
- Using Cisco pxGrid APIs
- Using Cisco Threat Grid APIs
- Investigating Cisco Umbrella Security Data Programmatically
- Exploring Cisco Umbrella Reporting and Enforcement APIs
- Automating Security with Cisco Firepower APIs
- Operationalizing Cisco Stealthwatch and the API Capabilities
- Using Cisco Stealthwatch Cloud APIs
- Describing Cisco Security Management Appliance APIs

TARGET AUDIENCE

- IT students and professionals seeking strong expertise in the subject and an internationally recognized qualification in the same for prospective jobs.
- Network security engineers seeking skill enrichment in network security technologies to nourish their passion and career.
- Aspirants in the following job profiles:

- Network Security Engineer
- Network Designer
- Network Administrator
- Consulting Systems Engineer
- Technical Solutions Architect
- Network Manager
- Cisco Integrators and partners

PREREQUISITES

- The CCNP Security does not require any particular qualification for attendance of the course. However, comprehensive knowledge of the subjects is necessary for attending the examinations.
- A CCNA certificate is not necessary. Students can appear for CCNP Security examinations if they have the equivalent theoretical and practical knowledge.
- Experience in networking field will be an advantage to attempt the CCNP examination.

LAB INFRASTRUCTURE

IP Rulers has a fully equipped lab, specially designed for the CCNP Security training, with an enhanced lab topology that represent real world network. Students will have the following equipment and software configured for their training; they may also get the chance to see newer hardware and software during this period.

EQUIPMENT AND SOFTWARE LIST

Virtual machines

- *Cisco Identity Services Engine (ISE): 2.4*
- *Cisco Web Security Appliance (WSA): 9.2*
- *Cisco Email Security Appliance (ESA): 11.1*
- *Cisco Firepower Management Center Virtual Appliance: 6.2*
- *Cisco Firepower NGIPSv: 6.2*
- *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: 6.10Cisco FireAMP Cloud: 5.3*
- *Cisco Wireless Controller (WLC): 8.3*
- *Cisco DNA Center Release 1.3.1*
- *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*

Others

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

TRAINER'S PROFILE

- IP Rulers is managed by an expert team of trainers with over ten 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

- Internationally valued certification from Cisco.
- ISpecialist Certification in any CCNP exam, whether it be core or concentration.
- Eligibility to attend the CCIE Security Lab Exam directly by passing the CCNP Core Examination.
- Constant acquaintance to the dynamic technologies in the IT field.
- Refreshment in regular concepts of Security Technologies along with Automation.
- Authority to link the CCNP 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

iprulers iprulers iprulers ip_rulers