

CCNP Security

To earn CCNP Security, pass two exams: a core exam and an enterprise concentration exam of your choice.

Core exam:

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

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)
- **300-715 SISE** Implementing and Configuring Cisco Identity Services Engine (SISE)
- **300-720 SESA** Securing Email with Cisco Email Security Appliance (SESA)
- **300-725 SWSA** Securing the Web with Cisco Web Security Appliance (SWSA)
- **300-730 SVPN** Implementing Secure Solutions with Virtual Private Networks (SVPN)
- **300-735 SAUTO** Implementing Automation for Cisco Security Solutions (SAUI)

Core (701-350 SCOR) Outlines

1- Security Concepts

- Explain common threats against on-premises and cloud environments
- Describe functions of the cryptography components such as hashing, encryption, PKI, SSL, IPsec, NAT-T IPv4 for IPsec, pre-shared key and certificate based authorization
- Explain the role of the endpoint in protecting humans from phishing and social engineering attacks
- Explain North Bound and South Bound APIs in the SDN architecture

2- Network Security

- Compare network security solutions that provide intrusion prevention and firewall capabilities
- Describe the components, capabilities, and benefits of NetFlow and Flexible NetFlow records
- Configure and verify network infrastructure security methods (router, switch, wireless)
- Implement management options for network security solutions such as intrusion prevention and perimeter security (Single vs. multidevice manager, in-band vs. out-of-band, CDP, DNS, SCP, SFTP, and DHCP security and risks)
- Configure AAA for device and network access (authentication and authorization, TACACS+, RADIUS and RADIUS flows, accounting, and dACL)
- Configure secure network management of perimeter security and infrastructure devices (secure device management, SNMPv3, views, groups, users, authentication, and encryption, secure logging, and NTP with authentication)
- Configure and verify site-to-site VPN and remote access VPN

CCNP Security

Core (701-350 SCOR) Outlines

3- Content Security

- Describe web proxy identity and authentication including transparent user identification
- Compare the components, capabilities, and benefits of local and cloud-based email and web solutions (ESA, CES, WSA)
- Configure and verify web and email security deployment methods to protect on-premises and remote users (inbound and outbound controls and policy management)
- Configure and verify email security features such as SPAM filtering, antimalware filtering, DLP, blacklisting, and email encryption
- Configure and verify secure internet gateway and web security features such as blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, and TLS decryption

4- Secure Network Access and Visibility

- Describe identity management and secure network access concepts such as guest services, profiling, posture assessment and BYOD
- Configure and verify network access device functionality such as 802.1X, MAB, WebAuth
- Describe network access with CoA
- Describe the benefits of device compliance and application control
- Describe the components, capabilities, and benefits of these security products and solutions (Cisco Stealthwatch and Cisco pxGrid)