CISCO 350-701

Cisco CCNP Security Certification Questions & Answers

Exam Summary – Syllabus – Questions

350-701

Cisco Certified Network Professional Security

90-110 Questions Exam – Variable (750-850 / 1000 Approx.) Cut Score – Duration of 120 minutes

Table of Contents:

Know Your 350-701 Certification Well:

The 350-701 is best suitable for candidates who want to gain knowledge in the Cisco Security. Before you start your 350-701 preparation you may struggle to get all the crucial CCNP Security materials like 350-701 syllabus, sample questions, study guide.

But don't worry the 350-701 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the 350-701 syllabus?
- How many questions are there in the 350-701 exam?
- Which Practice test would help me to pass the 350-701 exam at the first attempt?

Passing the 350-701 exam makes you Cisco Certified Network Professional Security. Having the CCNP Security certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

Cisco 350-701 CCNP Security Certification Details:

Exam Name	Implementing and Operating Cisco Security Core Technologies
Exam Code	350-701
Exam Price	$400 USD
Duration	120 minutes
Number of Questions	90-110
Passing Score	Variable (750-850 / 1000 Approx.)
Recommended Training	**Implementing and Operating Cisco Security Core Technologies (SCOR)**
Exam Registration	**PEARSON VUE**
Sample Questions	**Cisco 350-701 Sample Questions**
Practice Exam	**Cisco Certified Network Professional Security Practice Test**

350-701 Syllabus:

Section	Weight	Objectives
Security Concepts	25%	1. Explain common threats against on-premises and cloud environments • On-premises: viruses, trojans, DoS/DDoS attacks, phishing, rootkits, man-in-the-middle attacks, SQL injection, cross-site scripting, malware • Cloud: data breaches, insecure APIs, DoS/DDoS, compromised credentials 2. Compare common security vulnerabilities such as software bugs, weak and/or hardcoded passwords, SQL injection, missing encryption, buffer overflow, path traversal, cross-site scripting/forgery 3. 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 4. Compare site-to-site VPN and remote access VPN deployment types such as sVTI, IPsec, Cryptomap, DMVPN, FLEXVPN including high availability considerations, and AnyConnect 5. Describe security intelligence authoring, sharing, and consumption 6. Explain the role of the endpoint in protecting humans from phishing and social engineering attacks 7. Explain North Bound and South Bound APIs in the SDN architecture 8. Explain DNAC APIs for network provisioning, optimization, monitoring, and troubleshooting 9. Interpret basic Python scripts used to call Cisco Security appliances APIs
Network Security	20%	1. Compare network security solutions that provide intrusion prevention and firewall capabilities 2. Describe deployment models of network security solutions and architectures that provide intrusion prevention and firewall capabilities 3. Describe the components, capabilities, and benefits of NetFlow and Flexible NetFlow records 4. Configure and verify network infrastructure security methods (router, switch, wireless)

Section	Weight	Objectives
		• Layer 2 methods (Network segmentation using VLANs and VRF-lite; Layer 2 and port security; DHCP snooping; Dynamic ARP inspection; storm control; PVLANs to segregate network traffic; and defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks • Device hardening of network infrastructure security devices (control plane, data plane, management plane, and routing protocol security) 5. Implement segmentation, access control policies, AVC, URL filtering, and malware protection 6. 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) 7. Configure AAA for device and network access (authentication and authorization, TACACS+, RADIUS and RADIUS flows, accounting, and dACL) 8. 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) 9. Configure and verify site-to-site VPN and remote access VPN • Site-to-site VPN utilizing Cisco routers and IOS • Remote access VPN using Cisco AnyConnect Secure Mobility client • Debug commands to view IPsec tunnel establishment and troubleshooting
Securing the Cloud	15%	1. Identify security solutions for cloud environments • Public, private, hybrid, and community clouds • Cloud service models: SaaS, PaaS, IaaS (NIST 800-145) 2. Compare the customer vs. provider security responsibility for the different cloud service models • Patch management in the cloud • Security assessment in the cloud

Section	Weight	Objectives
		• Cloud-delivered security solutions such as firewall, management, proxy, security intelligence, and CASB 3. Describe the concept of DevSecOps (CI/CD pipeline, container orchestration, and security 4. Implement application and data security in cloud environments 5. Identify security capabilities, deployment models, and policy management to secure the cloud 6. Configure cloud logging and monitoring methodologies 7. Describe application and workload security concepts
Content Security	15%	1. Implement traffic redirection and capture methods 2. Describe web proxy identity and authentication including transparent user identification 3. Compare the components, capabilities, and benefits of local and cloud-based email and web solutions (ESA, CES, WSA) 4. Configure and verify web and email security deployment methods to protect on-premises and remote users (inbound and outbound controls and policy management) 5. Configure and verify email security features such as SPAM filtering, antimalware filtering, DLP, blacklisting, and email encryption 6. 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 7. Describe the components, capabilities, and benefits of Cisco Umbrella 8. Configure and verify web security controls on Cisco Umbrella (identities, URL content settings, destination lists, and reporting)
Endpoint Protection and Detection	10%	1. Compare Endpoint Protection Platforms (EPP) and Endpoint Detection & Response (EDR) solutions 2. Explain antimalware, retrospective security, Indication of Compromise (IOC), antivirus, dynamic file analysis, and endpoint-sourced telemetry 3. Configure and verify outbreak control and quarantines to limit infection 4. Describe justifications for endpoint-based security 5. Describe the value of endpoint device management and asset inventory such as MDM 6. Describe the uses and importance of a multifactor authentication (MFA) strategy

Section	Weight	Objectives
		7. Describe endpoint posture assessment solutions to ensure endpoint security 8. Explain the importance of an endpoint patching strategy
Secure Network Access, Visibility, and Enforcement	15%	1. Describe identity management and secure network access concepts such as guest services, profiling, posture assessment and BYOD 2. Configure and verify network access device functionality such as 802.1X, MAB, WebAuth 3. Describe network access with CoA 4. Describe the benefits of device compliance and application control 5. Explain exfiltration techniques (DNS tunneling, HTTPS, email, FTP/SSH/SCP/SFTP, ICMP, Messenger, IRC, NTP) 6. Describe the benefits of network telemetry 7. Describe the components, capabilities, and benefits of these security products and solutions • Cisco Stealthwatch • Cisco Stealthwatch Cloud • Cisco pxGrid • Cisco Umbrella Investigate • Cisco Cognitive Threat Analytics • Cisco Encrypted Traffic Analytics • Cisco AnyConnect Network Visibility Module (NVM)

Cisco 350-701 Sample Questions:

Question: 1

What are two list types within AMP for Endpoints Outbreak Control? (Choose two.)

a) blocked ports
b) simple custom detections
c) command and control
d) allowed applications

Answer: b, d

Question: 2

The Cisco ESA acts as a mail transfer agent. The Cisco ESA is the destination of which public records?

a) AA
b) MX
c) C-NAME
d) All of these answers are correct

Answer: b

Question: 3

In a PaaS model, which layer is the tenant responsible for maintaining and patching?

a) hypervisor
b) virtual machine
c) network
d) application

Answer: d

Question: 4

Cisco AMP for Endpoints has connectors for which of the following operating systems?

a) Windows
b) macOS
c) Android
d) All of these answers are correct

Answer: d

Question: 5

An authorization policy should always implement which of the following concepts? (Select all that apply.)

a) Implicit deny
b) Need to know
c) Access control debugging logs
d) Access control filter logs

Answer: a, b

Question: 6

You are hired to configure a site-to-site VPN between a Cisco FTD device and a Cisco IOS-XE router. Which of the following encryption and hashing protocols will you select for optimal security?

a) AES-192, SHA, Diffie-Hellman Group 21
b) IDEA, SHA, Diffie-Hellman Group 2
c) AES-192, SHA, Diffie-Hellman Group 5
d) AES-256, SHA, Diffie-Hellman Group 21

Answer: a

Question: 7

What are two Detection and Analytics Engines of Cognitive Threat Analytics? (Choose two.)

a) data exfiltration
b) command and control communication
c) intelligent proxy
d) snort
e) URL categorization

Answer: a, b

Question: 8

In which type of Cisco WSA deployment mode is the client configured to use the web proxy?

a) Transparent mode
b) Explicit forward mode
c) WCCP mode
d) None of these answers is correct

Answer: b

Question: 9

How does Cisco Stealthwatch Cloud provide security for cloud environments?

a) It facilitates secure connectivity between public and private networks.
b) It prevents exfiltration of sensitive data.
c) It delivers visibility and threat detection.
d) It assigns Internet-based DNS protection for clients and servers.

Answer: c

Question: 10

An MDM provides which two advantages to an organization with regards to device management?

(Choose two.)

a) critical device management
b) network device management
c) allowed application management
d) asset inventory management
e) Active Directory group policy management

Answer: a, c

Study Guide to Crack Cisco CCNP Security 350-701 Exam:

- Getting details of the 350-701 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 350-701 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Cisco provided training for 350-701 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 350-701 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 350-701 practice tests is must. Continuous practice will make you an expert in all syllabus areas.