CISCO 300-740

Cisco CCNP Security Certification Questions & Answers

Exam Summary – Syllabus – Questions

300-740

Cisco Certified Specialist Security Secure Cloud Access

55-65 Questions Exam – Variable (750-850 / 1000 Approx.) Cut Score – Duration of 90 minutes

Table of Contents:

Know Your 300-740 Certification Well:

The 300-740 is best suitable for candidates who want to gain knowledge in the Cisco Security. Before you start your 300-740 preparation you may struggle to get all the crucial CCNP Security materials like 300-740 syllabus, sample questions, study guide.

But don't worry the 300-740 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 300-740 syllabus?
- How many questions are there in the 300-740 exam?
- Which Practice test would help me to pass the 300-740 exam at the first attempt?

Passing the 300-740 exam makes you Cisco Certified Specialist Security Secure Cloud Access. 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 300-740 CCNP Security Certification Details:

Exam Name	Designing and Implementing Secure Cloud Access for Users and Endpoints
Exam Code	300-740
Exam Price	$300 USD
Duration	90 minutes
Number of Questions	55-65
Passing Score	Variable (750-850 / 1000 Approx.)
Recommended Training	**Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)**
Exam Registration	**PEARSON VUE**
Sample Questions	**Cisco 300-740 Sample Questions**
Practice Exam	**Cisco Certified Specialist Security Secure Cloud Access Practice Test**

300-740 Syllabus:

Section	Weight	Objectives
Cloud Security Architecture	10%	- Describe the components of the Cisco Security Reference Architecture • Threat intelligence • Security operations toolset • User/device security • Network security: cloud edge and on-premises • Workload, application, and data security - Describe use cases and the recommended capabilities within an integrated architecture • Common identity • Converged multicloud policy • SASE integrations • Zero-trust network access - Describe industry security frameworks such as NIST, CISA, and DISA - Describe the SAFE architectural framework - Describe the SAFE Key structure • Places in the Network • Secure Domains
User and Device Security	20%	- Implement user and device authentication via identity certificates • Implement multifactor authentication for users and devices • Implement endpoint posture policies for user access to resources • Configure SAML/SSO and OIDC using an identity provider connection • Configure user and device trust using SAML authentication for a mobile or web application
Network and Cloud Security	20%	- Determine security policies for endpoints to control access to cloud applications

Section	Weight	Objectives
		• URL filtering (web layer and DNS layer) • Advanced app control • Network protocol blocking such as FTP and bit torrent • Direct-internet-access for trusted business applications • Web application firewall • Reverse proxy - Determine security policies for endpoints to control access to SaaS applications such as Office 365, Workday, and Salesforce - Determine security policies for remote users using VPN or application-based - Determine security policies for network security edge to enforce application policy • Security services edge • Cisco Secure Firewall (FTD and ASA)
Application and Data Security	25%	- Describe the MITRE ATT&CK framework and attacker defense mitigation techniques - Describe cloud security attack tactics and mitigation strategies - Describe how web application firewalls protect against DDoS attacks - Determine security policies for application enforcement using Cisco Secure Workload and enforcement agents • Lateral movement prevention • Microsegmentation - Determine cloud (hybrid and multicloud) platform security policies based on application connectivity requirements (third- party providers such as AWS, Azure, and Google Cloud)
Visibility and Assurance	15%	- Describe the Cisco XDR solution - Describe use cases for visibility and assurance automation - Describe benefits and capabilities of visibility and logging tools such as SIEM, Open Telemetry, and Cisco

Section	Weight	Objectives
		Secure Network Analytics - Validate traffic flow and telemetry reports for baseline and compliance behavior analysis - Diagnose issues with user application and workload access • Cisco Secure Network Analytics • Cisco Secure Cloud Analytics • Cisco Secure Cloud Insights • Cisco Secure Analytics and Logging - Verify user access to applications and data using tools (firewall logs, Duo, Umbrella, and Cisco Secure Workload) - Analyze application dependencies using tools such as firewall logs and Cisco Secure Workload
Threat Response	10%	- Describe use cases for response automation - Determine actions based on telemetry reports - Determine policies based on security audit reports - Determine action based on user or application compromise • Contain • Report • Remediate • Reinstantiate

Cisco 300-740 Sample Questions:

Question: 1

For enforcing application policy at the network security edge, which of the following are critical?

a) Enforcing uniform policies without considering individual application requirements
b) Implementing dynamic security policies based on application behavior and user context
c) Ignoring encrypted traffic as it is considered secure
d) Integrating endpoint security for comprehensive network protection

Answer: b, d

Question: 2

To allow users a seamless and secure login experience across multiple applications, many organizations configure __________ using an identity provider connection.

a) firewalls
b) antivirus software
c) VPNs
d) SAML/SSO

Answer: d

Question: 3

Determine cloud platform security policies based on application connectivity requirements might involve:

a) Implementing network peering
b) Configuring firewalls and access lists
c) Selecting appropriate cloud service models (IaaS, PaaS, SaaS)
d) Avoiding the use of security groups and ACLs

Answer: a, b, c

Question: 4

Which security policy is most relevant for controlling access to SaaS applications like Office 365, Workday, and Salesforce?

a) Allowing all outbound traffic without inspection
b) Blocking all cloud services to ensure network security
c) Implementing access control based on user identity and device security posture
d) Unlimited data transfer policies

Answer: c

Question: 5

What are key considerations when implementing an integrated cloud security architecture?

a) Leveraging zero-trust principles
b) Ensuring compatibility between different cloud services
c) Centralizing all data storage on-premises
d) Implementing consistent security policies across environments

Answer: a, b, d

Question: 6

When determining security policies for application enforcement, which of the following is a key consideration?

a) The programming language used to develop the application
b) The popularity of the application among users
c) The color scheme of the application interface
d) The sensitivity of the data being accessed or stored by the application

Answer: d

Question: 7

Security services edge (SSE) combines which of the following services for enhanced security at the network edge?

a) Zero Trust Network Access (ZTNA)
b) Cloud Access Security Broker (CASB)
c) Secure Web Gateway (SWG)
d) Uninterruptible Power Supply (UPS)

Answer: a, b, c

Question: 8

In the context of network protocol blocking, which of the following statements is true?

a) All network protocols should be allowed to ensure maximum compatibility
b) Blocking protocols like FTP can prevent unauthorized data transfers
c) Protocol blocking is an outdated practice that reduces network efficiency
d) Blocking protocols like BitTorrent can limit the spread of malware

Answer: b, d

Question: 9

OIDC stands for OpenID Connect. What is it used for in the context of identity management?

a) To encrypt device data
b) To track user activity on websites
c) To authenticate users by leveraging an identity provider
d) To connect to open networks

Answer: c

Question: 10

_________ policies are crucial for restricting access to network resources based on the security health of a device.

a) Encryption
b) Endpoint posture
c) Password
d) Network segmentation

Answer: b

Study Guide to Crack CCNP Security 300-740 Exam:

- Getting details of the 300-740 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help.
- 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.
- Read from the 300-740 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 300-740 practice tests is must. Continuous practice will make you an expert in all syllabus areas.