300-208

Implementing Cisco Secure Access Solutions

NWExam.com

SUCCESS GUIDE TO CISCO CERTIFICATION

Exam Summary – Syllabus – Questions

Table of Contents

Introduction to 300-208 Exam on Implementing Cisco Secure Access Solutions

A great way to start the Cisco Certified Network Professional Security (SISAS) preparation is to begin by properly appreciating the role that syllabus and study guide play in the Cisco 300-208 certification exam. This study guide is an instrument to get you on the same page with Cisco and understand the nature of the Cisco CCNP Security exam.

Our team of experts has composed this Cisco 300-208 exam preparation guide to provide the overview about Cisco Implementing Cisco Secure Access Solutions exam, study material, sample questions, practice exam and ways to interpret the exam objectives to help you assess your readiness for the Cisco SISAS exam by identifying prerequisite areas of knowledge. We recommend you to refer the simulation questions and practice test listed in this guide to determine what type of questions will be asked and the level of difficulty that could be tested in the Cisco CCNP Security certification exam.

Cisco 300-208 Certification Details:

Exam Name	Implementing Cisco Secure Access Solutions
Exam Number	300-208 SISAS
Exam Price	$300 USD
Duration	90 minutes
Number of Questions	55-65
Passing Score	Variable (750-850 / 1000 Approx.)
Recommended Training	Implementing Cisco Secure Access Solutions - (SISAS)
Exam Registration	PEARSON VUE
Sample Questions	Cisco 300-208 Sample Questions
Practice Exam	**Cisco Certified Network Professional Security Practice Test**

Cisco 300-208 Exam Syllabus:

Section	Weight	Objectives
Identity Management/Secure Access	33%	1 Implement device administration a) Compare and select AAA options b) TACACS+ c) RADIUS d) Describe Native AD and LDAP 2 Describe identity management a) Describe features and functionality of authentication and authorization b) Describe identity store options (i.e., LDAP, AD, PKI, OTP, Smart Card, local) c) Implement accounting 3 Implement wired/wireless 802.1X a) Describe RADIUS flows b) AV pairs c) EAP types d) Describe supplicant, authenticator, and server e) Supplicant options f) 802.1X phasing (monitor mode, low impact, closed mode) g) AAA server h) Network access devices 4 Implement MAB a) Describe the MAB process within an 802.1X framework b) Flexible authentication configuration c) ISE authentication/authorization policies d) ISE endpoint identity configuration e) Verify MAB Operation 5 Implement network authorization enforcement a) dACL b) Dynamic VLAN assignment c) Describe SGA d) Named ACL e) CoA 6 Implement Central Web Authentication (CWA) a) Describe the function of CoA to support web authentication b) Configure authentication policy to facilitate CWA c) URL redirect policy d) Redirect ACL e) Customize web portal f) Verify central web authentication operation

Section	Weight	Objectives
		7 Implement profiling a) Enable the profiling services b) Network probes c) IOS Device Sensor d) Feed service e) Profiling policy rules f) Utilize profile assignment in authorization policies g) Verify profiling operation 8 Implement guest services a) Managing sponsor accounts b) Sponsor portals c) Guest portals d) Guest Policies e) Self registration f) Guest activation g) Differentiated secure access h) Verify guest services operation 9 Implement posture services a) Describe the function of CoA to support posture services b) Agent options c) Client provisioning policy and redirect ACL d) Posture policy e) Quarantine/remediation f) Verify posture service operation 10 Implement BYOD access a) Describe elements of a BYOD policy b) Device registration c) My devices portal d) Describe supplicant provisioning
Threat Defense	10%	1 Describe TrustSec Architecture a) SGT Classification - dynamic/static b) SGT Transport - inline tagging and SXP c) SGT Enforcement - SGACL and SGFW d) MACsec
Troubleshooting, Monitoring and Reporting Tools	7%	1 Troubleshoot identity management solutions a) Identify issues using authentication event details in Cisco ISE b) Troubleshoot using Cisco ISE diagnostic tools c) Troubleshoot endpoint issues d) Use debug commands to troubleshoot RADIUS and 802.1X on IOS switches and wireless controllers e) Troubleshoot backup operations

Section	Weight	Objectives
Threat Defense Architectures	17%	1 Design highly secure wireless solution with ISE a) Identity Management b) 802.1X c) MAB d) Network authorization enforcement e) CWA f) Profiling g) Guest Services h) Posture Services i) BYOD Access
Identity Management Architectures	33%	1 Device administration 2 Identity Management 3 Profiling 4 Guest Services 5 Posturing Services 6 BYOD Access

300-208 Sample Questions:

01. What shortcoming of the original RADIUS specification does CoA address?
a) Allows the AAA server to provide unsolicited authorization policy updates to AAA clients.
b) Allows co-authentication of the user and the endpoint.
c) Allows co-authorization on ingress device and egress device in Cisco TrustSec domain.
d) Change of address allows policy to follow user if they roam between wireless access points.
e) Allows RADIUS to be transported using TCP.

02. Which 802.1X mode uses a static pre-authentication ACL with a dynamically applied downloadable ACL after authentication?
a) Dynamic mode
b) Monitor mode
c) Multi-auth mode
d) Flexible enforcement mode
e) Low impact mode

03. What are three methods that Cisco ISE can use to perform authentication? (choose 3)
a) 802.1X
b) MAB
c) CoA
d) EAP
e) Active Directory
f) Web Authentication.

04. Which of the following is a benefit of EAP Chaining?
a) Multi-factor authentication
b) Two factor authentication
c) Specify user and machine details in authorization policy conditions
d) Outer EAP provides secure tunnel to protect inner EAP
e) Policy can consider both ingress identity and egress identity

05. Which of the following are roles that ISE plays in a Cisco TrustSec deployment?
(choose 2)
a) Distribute tags with SXP
b) Manage SGACLs
c) Map SGTs to VLANs
d) Dynamically assign SGTs to endpoints
e) Manage UCS port profiles

06. What component of ISE organizes attributes and their possible values which are used to define context sensitive policy conditions?
a) Vendor specific attribute
b) Contextual database
c) RADIUS
d) Dictionary
e) Directory

07. Which of the following must be configured on the switch to support Central Web Authentication? (choose 3)
a) Traffic filter ACL
b) Web redirection ACL
c) CoA
d) CTS
e) HTTP and HTTPS services
f) Redirection URL

08. Which of the following profiling probe functions are implemented directly in the NAD via the IOS Device-Sensor feature?
(choose 3)
a) NMAP
b) DNS
c) SNMPTrap
d) DHCP
e) CDP and LLDP
f) HTTP

09. Which of the following Cisco ISE features is associated with endpoint remediation?
a) Profiler
b) Authorization
c) Authentication
d) Posture
e) Guest services

10. Which element serves to maintain synchronization Cisco ISE and the NAD with respect to AAA activity for a particular endpoint?
a) MAC address
b) Common session ID
c) Endpoint handle
d) Security group tag
e) UID

Answers to 300-208 Exam Questions:

Question: 01 Answer: a	Question: 02 Answer: e	Question: 03 Answer: a, b, f	Question: 04 Answer: c	Question: 05 Answer: b, d
Question: 06 Answer: d	Question: 07 Answer: b, c, e	Question: 08 Answer: d, e, f	Question: 09 Answer: d	Question: 10 Answer: b

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@nwexam.com