Cisco 300-208 Syllabus

Exam Name	Implementing Cisco Secure Access Solutions
Exam Number	300-208 SISAS

Cisco Certified Network Professional Security

Identity Management/Secure Access

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

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

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

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

Threat Defense Architectures

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

1 Device administration

2 Identity Management

3 Profiling

4 Guest Services

5 Posturing Services

6 BYOD Access