Implementing Cisco Secure Access Solutions (300-208)

Exam Description: The Implementing Cisco Secure Access Solutions (SISAS) (300-208) exam tests whether a network security engineer knows the components and architecture of secure access, by utilizing 802.1X and Cisco TrustSec. This 90-minute exam consists of 65–75 questions and assesses knowledge of Cisco Identity Services Engine (ISE) architecture, solution, and components as an overall network threat mitigation and endpoint control solutions. It also includes the fundamental concepts of bring your own device (BYOD) using posture and profiling services of ISE. Candidates can prepare for this exam by taking the Implementing Cisco Secure Access Solutions (SISAS) course.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

33% 1.0 Identity Management and Secure Access

1.1 Implement device administration

1.1.a Compare and select AAA options

1.1.b TACACS+

1.1.c RADIUS

1.1.d Describe Native AD and LDAP

1.2 Describe identity management

1.2.a Describe features and functionality of authentication and authorization

1.2.b Describe identity store options (i.e., LDAP, AD, PKI, OTP, Smart Card, local)

1.2.c Implement accounting

1.3 Implement wired/wireless 802.1X

1.3.a Describe RADIUS flows

1.3.b AV pairs

1.3.c EAP types

1.3.d Describe supplicant, authenticator, and server

1.3.e Supplicant options

1.3.f 802.1X phasing (monitor mode, low impact, closed mode)

1.3.g AAA server

1.3.h Network access devices

1.4 Implement MAB

1.4.a Describe the MAB process within an 802.1X framework

1.4.b Flexible authentication configuration

1.4.c ISE authentication/authorization policies

1.4.d ISE endpoint identity configuration

1.4.e Verify MAB Operation

1.5 Implement network authorization enforcement

- 1.5.a dACL
- 1.5.b Dynamic VLAN assignment
- 1.5.c Describe SGA
- 1.5.d Named ACL
- 1.5.e CoA

1.6 Implement Central Web Authentication (CWA)

- 1.6.a Describe the function of CoA to support web authentication
- 1.6.b Configure authentication policy to facilitate CWA
- 1.6.c URL redirect policy
- 1.6.d Redirect ACL
- 1.6.e Customize web portal
- 1.6.f Verify central web authentication operation

1.7 Implement profiling

- 1.7.a Enable the profiling services
- 1.7.b Network probes
- 1.7.c IOS Device Sensor
- 1.7.d Feed service
- 1.7.e Profiling policy rules
- 1.7.f Utilize profile assignment in authorization policies
- 1.7.g Verify profiling operation

1.8 Implement guest services

- 1.8.a Managing sponsor accounts
- 1.8.b Sponsor portals
- 1.8.c Guest portals
- 1.8.d Guest Policies
- 1.8.e Self registration
- 1.8.f Guest activation
- 1.8.g Differentiated secure access
- 1.8.h Verify guest services operation

1.9 Implement posture services

- 1.9.a Describe the function of CoA to support posture services
- 1.9.b Agent options
- 1.9.c Client provisioning policy and redirect ACL
- 1.9.d Posture policy
- 1.9.e Quarantine/remediation
- 1.9.f Verify posture service operation

1.10 Implement BYOD access

- 1.10.a Describe elements of a BYOD policy
- 1.10.b Device registration
- 1.10.c My devices portal

1.10.d Describe supplicant provisioning

10% 2.0 Threat Defense

2.1 Describe TrustSec Architecture

2.1.a SGT Classification – dynamic/static

2.1.b SGT Transport – inline tagging and SXP

2.1.c SGT Enforcement – SGACL and SGFW

2.1.d MACsec

7% 3.0 Troubleshooting, Monitoring, and Reporting Tools

3.1 Troubleshoot identity management solutions

3.1.a Identify issues using authentication event details in Cisco ISE

3.1.b Troubleshoot using Cisco ISE diagnostic tools

3.1.c Troubleshoot endpoint issues

3.1.d Use debug commands to troubleshoot RADIUS and 802.1X on IOS switches and wireless controllers

3.1.e Troubleshoot backup operations

17% 4.0 Threat Defense Architectures

4.1 Design highly secure wireless solution with ISE

4.1.a Identity Management

4.1.b 802.1X

4.1.c MAB

4.1.d Network authorization enforcement

4.1.e CWA

4.1.f Profiling

4.1.g Guest Services

4.1.h Posture Services

4.1.i BYOD Access

33% 5.0 Design Identity Management Architectures

5.1 Device administration

5.2 Identity Management

5.3 Profiling

5.4 Guest Services

5.5 Posturing Services

5.6 BYOD Access