Implementing Cisco Secure Access Solutions **(300-208)**

Exam Description: The 300-208 Implementing Cisco Secure Access Solutions (SISAS) 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 55 – 65 questions. It tests on 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 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/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, 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
- 1.5 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 authorization

1.7 Implement profiling

1.8 Implement guest services

1.9 Implement posturing

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 Implement firewall

- 2.1.a Describe SGA ACLs

7% 3.0 Troubleshooting, Monitoring, and Reporting Tools

3.1 Troubleshoot identity management solutions

17% 4.0 Threat Defense Architectures

4.1 Design highly secure wireless solution

33% 5.0 Identity Management Architectures

5.1 Design AAA security solution

5.2 Design profiling security solution

5.3 Design posturing security solution

5.4 Design BYOD security solution

5.5 Design device admin security solution

5.6 Design guest services security solution