Implementing Cisco Secure Mobility Solutions (300-209)

Exam Description:

The Implementing Cisco Secure Mobility Solutions (SIMOS) (300-209) exam tests a network security engineer on the variety of Virtual Private Network (VPN) solutions that Cisco has available on the Cisco ASA firewall and Cisco IOS software platforms. This 90-minute exam consists of 65–75 questions and assesses the knowledge necessary to properly implement highly secure remote communications through VPN technology, such as remote access SSL VPN and site-to-site VPN (DMVPN, FlexVPN). Candidates can prepare for this exam by taking the Implementing Cisco Secure Mobility Solutions (SIMOS) 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.

1.0 Secure Communications

1.1 Site-to-site VPNs on routers and firewalls

- 1.1.a Describe GETVPN
- 1.1.b Implement IPsec (with IKEv1 and IKEv2 for both IPV4 & IPV6)
- 1.1.c Implement DMVPN (hub-Spoke and spoke-spoke on both IPV4 & IPV6)
- 1.1.d Implement FlexVPN (hub-Spoke on both IPV4 & IPV6) using local AAA

1.2 Implement remote access VPNs

- 1.2.a Implement AnyConnect IKEv2 VPNs on ASA and routers
- 1.2.b Implement AnyConnect SSLVPN on ASA and routers
- 1.2.c Implement clientless SSLVPN on ASA and routers
- 1.2.d Implement FLEX VPN on routers

2.0 Troubleshooting, Monitoring and Reporting Tools (as implemented above)

2.1 Troubleshoot VPN using ASDM & CLI

- 2.1.a Troubleshoot IPsec
- 2.1.b Troubleshoot DMVPN
- 2.1.c Troubleshoot FlexVPN
- 2.1.d Troubleshoot AnyConnect IKEv2 and SSL VPNs on ASA and routers
- 2.1.e Troubleshoot clientless SSLVPN on ASA and routers

2.0 Troubleshooting, Monitoring and Reporting Tools (as implemented above)

2.1 Troubleshoot VPN using ASDM & CLI

- 2.1.a Troubleshoot IPsec
- 2.1.b Troubleshoot DMVPN
- 2.1.c Troubleshoot FlexVPN
- 2.1.d Troubleshoot AnyConnect IKEv2 and SSL VPNs on ASA and routers
- 2.1.e Troubleshoot clientless SSLVPN on ASA and routers

3.0 Secure Communication Architectures

3.1 Design site-to-site VPN solutions

- 3.1.a Identify functional components of GETVPN, FlexVPN, DMVPN, and IPsec
- 3.1.b VPN technology considerations based on functional requirements
- 3.1.c High availability considerations
- 3.1.d Identify VPN technology based on configuration output

3.2 Design remote access VPN solutions

- 3.2.a Identify functional components of FlexVPN, IPsec, and Clientless SSL
- 3.2.b VPN technology considerations based on functional requirements
- 3.2.c High availability considerations
- 3.2.d Identify VPN technology based on configuration output
- 3.2.e Identify AnyConnect client requirements
- 3.2.f Clientless SSL browser and client considerations/requirements
- 3.2.g Identify split tunnelling requirements

3.3 Describe encryption, hashing, and Next Generation Encryption (NGE)

- 3.3.a Compare and contrast Symmetric and asymmetric key algorithms
- 3.3.b Identify and describe the cryptographic process in VPNs – Diffie Hellman, IPsec – ESP, AH, IKEv1, IKEv2, hashing algorithms MD5 and SHA, and authentication methods
- 3.3.c Describe PKI components and protection methods
- 3.3.d Describe Elliptic Curve Cryptography (ECC)
- 3.3.e Compare and contrast SSL, DTLS, and TLS