Securing Cisco Wireless Enterprise Networks (300-375)

Exam Description: The 300-375 Securing Wireless Enterprise Networks (WISECURE) exam is a 90-minute, 60-70 question assessment that is associated with the CCNP Wireless certification. This exam tests a candidate's knowledge of implementing client device security, identity based authentication and services, along with securing and monitoring the Enterprise wireless infrastructure. Candidates can prepare for this exam by taking the Securing Wireless Enterprise Networks (WISECURE) course.

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

19% 1.0 Integrate Client Device Security

1.1. Describe Extensible Authentication Protocol (EAP) authentication process

1.2. Configure client for secure EAP authentication
- 1.2.a. Native OS (iOS, Android, Windows, MAC OS, year 2013+) or AnyConnect client

1.3. Describe the impact of security configurations on application and client roaming
- 1.3.a. Key caching
- 1.3.b. 802.11r

1.4. Implement 802.11w Protected Management Frame (PMF) on the WLAN
- 1.4.a. Client support
- 1.4.b. PMF modes
- 1.4.c. Relevant timer settings

1.5. Implement Cisco Management Frame Protection (MFP)
- 1.5.a. Cisco Compatible Extensions (CCX)
- 1.5.b. Infrastructure mode
- 1.5.c. Client and infrastructure mode

1.6. Describe and configure client profiling
- 1.6.a. ISE
- 1.6.b. WLC

24% 2.0 Implement Secure Distribution System Connectivity Services on the Wireless Infrastructure

2.1. Describe the impact of BYOD on wireless security
- 2.1.a Additional security risks
- 2.1.b Loss of device control
- 2.1.c Increased complexity of policy enforcement

2.2. Implement BYOD policies
- 2.2.a. Single vs dual SSID
- 2.2.b. Self registration
- 2.2.c. mDNS sharing
- 2.2.d. Wi-Fi Direct

2.3. Implement AAA based Layer 3 security on the controller
- 2.3.a. Local Web Auth (LWA)
  - 2.3.a.1. External authentication)
  - 2.3.a.2. Locally significant certificates
  - 2.3.a.3. Pre-authentication ACL
  - 2.3.a.4. Pass through configuration

2.4. Describe regulatory compliance considerations for protecting data and access and providing accountability
- 2.4.a. PCI

2.5. Utilize security audit tools for Distribution Systems
- 2.5.a. PI reports
- 2.5.b. PCI audit

27% 3.0 Implement Secure Client Connectivity Services on the Wireless Infrastructure

3.1. Implement 802.1x wireless client authentication
- 3.1.a. AireOS
  - 3.1.a.1. Local
  - 3.1.a.2. Central
- 3.1.b. IOS-XE
- 3.1.c. Autonomous
  - 3.1.c.1. Local authentication
  - 3.1.c.2. Remote authentication
- 3.1.d. FlexConnect
  - 3.1.d.1. Local authentication
  - 3.1.d.2. Remote authentication

3.2. Implement Identity Based Networking (IBN)
- 3.2.a. AireOS
  - 3.2.a.1. VLANs
  - 3.2.a.2. QoS
  - 3.2.a.3. ACLs
- 3.2.b. IOS-XE
  - 3.2.b.1. VLANs
  - 3.2.b.2. QoS
  - 3.2.b.3. ACLs
- 3.2.c. Autonomous

3.2.c.1. VLAN
3.2.d. FlexConnect
3.2.d.1. VLAN
3.2.d.2. ACLs
3.2.d.3. QoS

3.3. Implement ISE AAA parameters for integration with the wireless network
3.3.a. Network device
3.3.b. IBN profile

3.4. Implement AAA based Layer 3 security using ISE
3.4.a. Utilizing ISE as AAA service
3.4.a.1. Locally significant certificates on ISE
3.4.a.2. Using captive portal capabilities for guest access
3.4.b. Central Web Auth (CWA
3.4.b.1. Returned values and overrides
3.4.b.2. Access accept
3.4.b.3. AAA override statement

3.5. Configure MSE based web authentication

3.6. Utilize security audit tools for client connectivity
3.6.a. PI reports
3.6.b. PCI audit

14% 4.0 Implement Secure Management Access on the WLAN Infrastructure

4.1. Controlling administrative access to the wireless infrastructure
4.1.a. RADIUS
4.1.b. TACACS
4.1.c. Controller and ISE integration
4.1.d. Access point administration credentials

4.2. Configure APs and switches for 802.1x access to the wired infrastructure
4.2.a. Controller based
4.2.b. Autonomous

4.3. Implement SNMPv3 on the wireless infrastructure
4.3.a. AireOS
4.3.b. IOS-XE
4.3.c. Autonomous

16% 5.0 Monitoring Security on the WLAN Infrastructure

5.1. Execute Security reports on PI

5.2. Perform Rogue Management

- 5.2.a. Rogue Containment on WLC and PI
- 5.2.b. RLDP on WLC and PI
- 5.2.c. SwitchPort tracing on PI
- 5.2.d. Location on PI
- 5.2.e. Rogue Rules on WLC and PI

5.3. Monitor rogue APs and clients
- 5.3.a. PI Maps
- 5.3.b. Controller

5.4. Monitor Alarms
- 5.4.a. 2 items
- 5.4.b. PI Security Tab
- 5.4.c. Controller Trap Logs

5.5. Identify RF related Security interferers on WLC and PI Maps
- 5.5.a. Jammers
- 5.5.b. Inverted Wi-Fi
- 5.5.c. Wi-Fi invalid channel

5.6. Implement wIPS
- 5.6.a. Enhanced Local Mode (ELM)