Implementing Advanced Cisco Unified Wireless Security (642-737)

Exam Description: The Implementing Advanced Cisco Unified Wireless Security (IAUWS) version 2.0 642-737 exam is a 90-minute test with 55−75 questions that are associated with the Cisco CCNP® Wireless certification. This exam assesses a candidate's ability to secure the wireless network from security threats via appropriate security policies and best practices, properly implement security standards, and properly configure wireless security components. The exam is closed book and no outside reference materials are allowed.

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.

22% 1.0 Integrate Client Device Security

- 1.1 Describe the EAP authentication process
- 1.2 Configure client for secure EAP authentication
- 1.3 Configure the Cisco any connect client
- 1.4 Describe the impact of security configurations on application and client roaming
- 1.5 Troubleshoot client wireless authentication issues
  - 1.5.a Packet analyzers
  - 1.5.b Debugs
  - 1.5.c Logs
  - 1.5.d Cisco WCS
  - 1.5.e ACS
- 1.6 Identify client security risks
  - 1.6.a Driver update
  - 1.6.b MS hot fixes

11% 2.0 Design and Integrate Wireless Network with NAC

- 2.1 Describe the architectures
  - 2.1.a In-band
  - 2.1.b Out-of-band
  - 2.1.c Agent versus agentless
  - 2.1.d Cisco NAC appliance
- 2.2 Describe the high-level authentication process flow

2.2.a CAS
2.2.b CAM
2.2.c RADIUS/ACS
2.2.d WLC
2.2.e External authentication sources

2.3 Configure the WLC for the NAC

2.4 Verify wireless authentication with NAC

22% 3.0 Implement Secure Wireless Connectivity Services

3.1 Configure authentication
3.1.a Controller local EAP with or without external
3.1.b LDAP database
3.1.c Client authentication on H-REAP APs
3.1.d 802.1X authentication for AP authentication to the switch

3.2 Configure autonomous AP for RADIUS authentication

3.3 Configure management frame protection on clients, APs, and controllers

3.4 Configure IBN
3.4.a RADIUS-based VLAN and ACLs
3.4.b AAA override

3.5 Define ACS parameters for integration with wireless network

3.6 Define client and server-side digital certificate requirements

3.7 Implement ACLs on controller
3.7.a CPU ACLs
3.7.b WLAN, interface, and client identity ACL

3.8 Troubleshoot secure wireless connectivity services
3.8.a Packet analyzers, debugs, logs, WCS, and ACS
3.8.b Verify firewall ports
3.8.c ACS and controller authorization and authentication for clients

12% 4.0 Design and Implement Guest Access Services

4.1 Describe the architectures for guest access services
4.1.a VLAN-based
4.1.b Anchor, DMZ, redundancy, and scaling
4.1.c NAC guest server
4.1.d Wired guest access
4.1.e Bandwidth limiting

4.2 Configure guest access accounts
4.2.a Lobby ambassador (controller and WCS-based)

4.2.b Guest roles

4.3 Configure controller web authentication
- 4.3.a Pass-through
- 4.3.b Internal and external
- 4.3.c Authentication (local/RADIUS)
- 4.3.d Custom splash page (internal, external, and per WLAN)
- 4.3.e Understand design considerations (DNS, proxy)
- 4.3.f Pre-authentication ACL
- 4.3.g Wired guest access
- 4.3.h Install third-party certificate on controller

4.4 Configure the anchor and internal controllers

4.5 Troubleshoot guest access issues
- 4.5.a Packet analyzers, debugs, logs, WCS, and ACS
- 4.5.b Verify firewall ports
- 4.5.c Mping and eping
- 4.5.d Proxies

11% 5.0 Translate Organizational and Regulatory Security Policies and Enforce Security Compliance

5.1 Describe regulatory compliance considerations
- 5.1.a HIPAA
- 5.1.b PCI
- 5.1.c SOX
- 5.1.d FERPA

5.2 Segment traffic into different VLANs, based upon these functions:
- 5.2.a Security
- 5.2.b Application
- 5.2.c QoS

5.3 Configure administration security on controller and WCS
- 5.3.a TACACS+ and ACS integration
- 5.3.b Local
- 5.3.c RADIUS and AAA server integration
- 5.3.d Access point administration credential
- 5.3.e Admin roles

5.4 Manage WLC and WCS alarms
- 5.4.a SNMP and trap receivers
- 5.4.b Syslog
- 5.4.c SMTP
- 5.4.d ACS log
- 5.4 e Modify WCS alarm levels

5.5 Utilize security audit tools

5.5.a Packet captures
5.5.b Penetration testing
5.5.c Third-party software (air magnet, air wise)
5.5.d PCI audit tool in WCS

11% 6.0 Configure Native WLC Security Feature Sets: IPS/IDS

6.1 Utilize WCS or controller for IDS and threat mitigation strategies
- 6.1.a Signature
- 6.1.b Custom signature
- 6.1.c Rogue classification management and (auto) containment
- 6.1.d Rogue reporting and location (WCS only)
- 6.1.e Switch port tracing (WCS only)
- 6.1.f Integrate Cisco spectrum expert with WCS
- 6.1.g Client exclusion
- 6.1.h Clean air

6.2 Identify and mitigate wireless vulnerabilities
- 6.2.a Wireless packet injection (can't be mitigated)
- 6.2.b Client misconfiguration
- 6.2.c DoS (RF jamming)
- 6.2.d Anomalous behavior attacks (association and authentication attacks)
- 6.2.e Signature attacks (net stumbler and undetectable at this time)
- 6.2.f Eavesdropping (wild packets and honeypot)
- 6.2.g Hijacking and mimicry (evil twin and honey potting)
- 6.2.h Social engineering (human attack)

11% 7.0 Integrate Wireless Network with Advanced Security Platforms

7.1 Describe Cisco end-to-end security solutions and how they integrate with Cisco wireless solutions
- 7.1.a any connect 3.0 and above
- 7.1.b NAC appliance
- 7.1.c NAC guest server
- 7.1.d Wired IPS
- 7.1.e ACS

7.2 Describe the Cisco unified wireless network firewall port configuration requirements
- 7.2.a ACLs
- 7.2.b IP port pass-through
- 7.2.c DMZ

7.3 Configure the controller for wired IPS and IDS

7.4 Configure wireless intrusion prevention system (MSE)