Cisco

Exam 300-375

Securing Wireless Enterprise Networks

Verson: Demo

[Total Questions: 10]

Question No : 1

A network engineer is implementing a wireless network and is considering deploying a single SSID for device onboarding. Winch option is a benefit of using dual SSIDs with a captive portal on the onboard SSID compared to a single SSID solution?

A. limit of a single device per user
B. restrict allowed devices types
C. allow multiple devices per user
D. minimize client configuration errors

Answer: B

Question No : 2

A customer is concerned about DOS attacks from a neighboring facility. Which feature can be enabled to help alleviate these concerns and mitigate DOS attacks on a WLAN?

A. PMF
B. peer-to-peer blocking
C. Cisco Centralized Key Management
D. split tunnel

Answer: A

Question No : 3

Refer to the exhibit.

What is the 1.1.1.1 IP address?

A. the wireless client IP address
B. the RADIUS server IP address
C. the controller management IP address
D. the lightweight IP address
E. the controller AP-manager IP address
F. the controller virtual interface IP address

Answer: F

Question No : 4

Which feature should an engineer select to implement the use of VLAN tagging, QoS, and ACLs to clients based on RADIUS attributes?

A. per-WLAN RADIUS source support
B. client profiling
C. AAA override
D. captive bypassing
E. identity-based networking

Answer: C

Question No : 5

What are two of the benefits that the Cisco AnyConnect v3.0 provides to the administrator for client WLAN security configuration? (Choose two.)

A. Provides a reporting mechanism for rouge APs
B. Prevents a user from adding any WLANs
C. Hides the complexity of 802.1X and EAP configuration
D. Supports centralized or distributed client architectures
E. Provides concurrent wired and wireless connectivity
F. Allows users to modify but not delete admin-created profiles

Answer: C,D

Question No : 6

After receiving an alert regarding a rogue AP, a network engineer logs into Cisco Prime and looks at the floor map where the AP that detected the rogue is located. The map is synchronized with a mobility services engine that determines the rogue device is actually inside the campus. The engineer determines the rogue to be a security threat and decides to stop it from broadcasting inside the enterprise wireless network. What is the fastest way to disable the rogue?

A. Go to the location the rogue device is indicated to be and disable the power.
B. Create an SSID on WLAN controller resembling the SSID of the rogue to spoof it and disable clients from connecting to it.
C. Classify the rogue as malicious in Cisco Prime.
D. Update the status of the rogue in Cisco Prime to contained.

Answer: C

Question No : 7

Which command is an SNMPv3-specific command that an engineer can use only in Cisco IOS XE?

A. snmp-server user remoteuser1 group1 remote 10.12.0.4
B. snmp-server host 172.16.1.33 public
C. snmp-server community comaccess ro 4
D. snmp-server enable traps wireless

Answer: A

Question No : 8

What two actions must be taken by an engineer configuring wireless Identity-Based Networking for a WLAN to enable VLAN tagging? (Choose two.)

A. enable AAA override on the WLAN
B. create and apply the appropriate ACL to the WLAN
C. update the RADIUS server attributes for tunnel type 64, medium type 65, and tunnel private group type 81

D. configure RADIUS server with WLAN subnet and VLAN ID
E. enable VLAN Select on the wireless LAN controller and the WLAN

Answer: A,C

Question No : 9

Which client roam is considered the fastest in a wireless deployment using Cisco IOS XE mobility controllers and mobility agents?

A. Roam within stack members
B. Inlet-SPG roam
C. Interdomain roam
D. Intermobility roam
E. Intra-SPG roam

Answer: E

Question No : 10

Clients are failing EAP authentication. A debug shows that an EAPOL start is sent and the clients are then de-authenticated. Which two issues can cause this problem? (Choose two.)

A. The WLC certificate has changed.
B. The WLAN is not configured for the correct EAP supplicant type.
C. The shared secret of the WLC and RADIUS server do not match.
D. The WLC has not been added to the RADIUS server as a client.
E. The clients are configured for machine authentication, but the RADIUS server is configured for user authentication.

Answer: C,D