

Fortinet

Exam Questions NSE6_FWF-6.4

Fortinet NSE 6 - Secure Wireless LAN 6.4



NEW QUESTION 1

Which two statements about background rogue scanning are correct? (Choose two.)

- A. A dedicated radio configured for background scanning can support the connection of wireless clients
- B. When detecting rogue APs, a dedicated radio configured for background scanning can suppress the rogue AP
- C. Background rogue scanning requires DARRP to be enabled on the AP instance
- D. A dedicated radio configured for background scanning can detect rogue devices on all other channels in its configured frequency band

Answer: CD

NEW QUESTION 2

When configuring a wireless network for dynamic VLAN allocation, which three IETF attributes must be supplied by the radius server? (Choose three.)

- A. 81 Tunnel-Private-Group-ID
- B. 65 Tunnel-Medium-Type
- C. 83 Tunnel-Preference
- D. 58 Egress-VLAN-Name
- E. 64 Tunnel-Type

Answer: ABE

Explanation:

The RADIUS user attributes used for the VLAN ID assignment are: IETF 64 (Tunnel Type)—Set this to VLAN.

IETF 65 (Tunnel Medium Type)—Set this to 802

IETF 81 (Tunnel Private Group ID)—Set this to VLAN ID.

NEW QUESTION 3

Refer to the exhibits.

Exhibit A

```
53836.574 xx:xx:xx:xx:xx:xx <ih> IEEE 802.11 mgmt::assoc_req <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rId 1 wId2
yy:yy:yy:yy:yy:yy

53836.574 xx:xx:xx:xx:xx:xx <ih> xx:xx:xx:xx:xx:xx sta =
0x6311c88, sta->flags = 0x00000001, auth_alg = 0, hapd->splitMac: 1

53836.575 xx:xx:xx:xx:xx:xx <ih> IEEE 802.11 mgmt::assoc_resp <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rId 1 wId2
yy:yy:yy:yy:yy:yy

53836.575 xx:xx:xx:xx:xx:xx <ih> IEEE 802.11 mgmt::assoc_resp <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rId 1 wId2
yy:yy:yy:yy:yy:yy

53836.575 xx:xx:xx:xx:xx:xx <dc> STA add xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId2 bssid
yy:yy:yy:yy:yy:yy NON-AUTH band 0x10 mimo 2*2

53836.575 xx:xx:xx:xx:xx:xx <cc> STA_CFG_REQ(10) sta
xx:xx:xx:xx:xx:xx add ==> ws (0-192.168.5.98:5246) rId 1 wId 2

53836.576 xx:xx:xx:xx:xx:xx <cc> STA add xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId 2 yy:yy:yy:yy:yy:yy sec
WPA2 PERSONAL auth 0

53836.576 xx:xx:xx:xx:xx:xx cwAcStaRbtAdd: I2C_STA_ADD insert sta
xx:xx:xx:xx:xx:xx 192.168.5.98/1/2/1

53836.577 xx:xx:xx:xx:xx:xx <cc> STA_CFG_RESP(10) sta xx:xx:xx:xx:xx:xx
<== ws (0-192.168.5.98:5246) rc 0 (Success)

64318.579 xx:xx:xx:xx:xx:xx <eh> RADIUS message (type=0) ==> RADIUS
Server code=1 (Access-Request) id=9 len=214

64318.579 xx:xx:xx:xx:xx:xx <eh> send 1/4 msg of 4-Way
Handshake

64318.580 xx:xx:xx:xx:xx:xx <eh> send IEEE 802.1X ver=2 type=3
(EAPOL_KEY) data len=95 replay cnt 1

64813.580 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL99B) ==>
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId 2
yy:yy:yy:yy:yy:yy

64318.582 xx:xx:xx:xx:xx:xx <eh> RADIUS message (type=0) <== RADIUS
Server code=2 (Access-Accept) id=9 len=114

53836.582 xx:xx:xx:xx:xx:xx <dc> STA chg xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId 2 bssid
yy:yy:yy:yy:yy:yy Auth:allow
```

Exhibit B

```

64813.583 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 121B) <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.583 xx:xx:xx:xx:xx:xx <eh>      recv IEEE 802.1X ver=1 type=3
(EAPOL_KEY) data len=117

64813.583 xx:xx:xx:xx:xx:xx <eh>      recv EAPOL-Key 2/4 Pairwise
replay cnt 1

64813.583 xx:xx:xx:xx:xx:xx <eh>      send 3/4 msg of 4-Way
Handshake

64813.584 xx:xx:xx:xx:xx:xx <eh>      send IEEE 802.1X ver=2 type=3
(EAPOL_KEY) data len=151 replay cnt 2

64813.584 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 155B) ==>
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.586 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 99B) <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.586 xx:xx:xx:xx:xx:xx <eh>      recv IEEE 802.1X ver=1 type=3
(EAPOL_KEY) data len=35

64813.586 xx:xx:xx:xx:xx:xx <eh>      recv EAPOL-Key 4/4 Pairwise
replay cnt 2

53836.587 xx:xx:xx:xx:xx:xx <dc> STA chg xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId2 bssid
yy:yy:yy:yy:yy:yy AUTH

53836.587 xx:xx:xx:xx:xx:xx <cc> STA chg xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId2 yy:yy:yy:yy:yy:yy sec
WPA2 PERSONAL auth 1 *****

53836.587 xx:xx:xx:xx:xx:xx <cc> STA_CFG_REQ(12) sta
xx:xx:xx:xx:xx:xx add key (len=16) ==> ws (0-192.168.5.98:5246) rId
1 wId2

53836.589 xx:xx:xx:xx:xx:xx <cc> STA_CFG_REQ(12) xx:xx:xx:xx:xx:xx
<== ws (0-192.168.5.98:5246) rc 0 (Success)

53837.140 xx:xx:xx:xx:xx:xx <dc> DHCP Request server 0.0.0.0 <==
host DESKTOP-CVKGHH mac xx:xx:xx:xx:xx:xx ip 192.168.30.2 xId
88548005

53837.142 xx:xx:xx:xx:xx:xx <dc> DHCP Ack server 192.168.30.1 ==>
host mac xx:xx:xx:xx:xx:xx ip 192.168.30.2 mask 255.255.255.0 gw
192.168.30.1 xId 88548005

```

The exhibits show the diagnose debug log of a station connection taken on the controller CLI. Which security mode is used by the wireless connection?

- A. WPA2 Enterprise
- B. WPA3 Enterprise
- C. WPA2 Personal and radius MAC filtering
- D. Open, with radius MAC filtering

Answer: C

NEW QUESTION 4

Which two configurations are compatible for Wireless Single Sign-On (WSSO)? (Choose two.)

- A. A VAP configured for captive portal authentication
- B. A VAP configured for WPA2 or 3 Enterprise
- C. A VAP configured to authenticate locally on FortiGate

D. A VAP configured to authenticate using a radius server

Answer: BD

Explanation:

In the SSID choose WPA2-Enterprise authentication.

WSSO is RADIUS-based authentication that passes the user's user group memberships to the FortiGate.

NEW QUESTION 5

Where in the controller interface can you find a wireless client's upstream and downstream link rates?

- A. On the AP CLI, using the cw_diag ksta command
- B. On the controller CLI, using the diag wireless-controller wlac -d sta command
- C. On the AP CLI, using the cw_diag -d sta command
- D. On the controller CLI, using the WiFi Client monitor

Answer: A

NEW QUESTION 6

A tunnel mode wireless network is configured on a FortiGate wireless controller. Which task must be completed before the wireless network can be used?

- A. The wireless network interface must be assigned a Layer 3 address
- B. Security Fabric and HTTPS must be enabled on the wireless network interface
- C. The wireless network to Internet firewall policy must be configured
- D. The new network must be manually assigned to a FortiAP profile.

Answer: C

Explanation:

A FortiGate unit is an industry leading enterprise firewall. In addition to consolidating all the functions of a network firewall, IPS, anti-malware, VPN, WAN optimization, Web filtering, and application control in a single platform, FortiGate also has an integrated Wi-Fi controller.

NEW QUESTION 7

Refer to the exhibit.

Radio 2

Mode

DisabledAccess PointDedicated Monitor

WIDS profile

default-wids-apscan-enabled

Radio resource provision

Band

5 GHz802.11ac/n/a

Channel width

20MHz40MHz80MHz

Short guard interval

Channels

✓

36

✓

40

✓

44

✓

48

✓

52*

✓

56*

✓

60*

✓

64*

✓

100*

✓

104*

✓

108*

✓

112*

✓

116*

✓

120*

✓

124*

✓

128*

✓

132*

✓

136*

✓

140*

✓

144*

✓

149

✓

153

✓

157

✓

161

✓

165

TX power control

AutoManual

TX power

10

—

17

dBm

SSIDs

(()) Tunnel

Bridge

Manual

Monitor channel utilization

What does the asterisk (*) symbol beside the channel mean?

- A. Indicates channels that can be used only when Radio Resource Provisioning is enabled

- B. Indicates channels that cannot be used because of regulatory channel restrictions
- C. Indicates channels that will be scanned by the Wireless Intrusion Detection System (WIDS)
- D. Indicates channels that are subject to dynamic frequency selection (DFS) regulations

Answer: D

NEW QUESTION 8

As a network administrator, you are responsible for managing an enterprise secure wireless LAN. The controller is based in the United States, and you have been asked to deploy a number of managed APs in a remote office in Germany.

What is the correct way to ensure that the RF channels and transmission power limits are appropriately configured for the remote APs?

- A. Configure the APs individually by overriding the settings in Managed FortiAPs
- B. Configure the controller for the correct country code for Germany
- C. Clone a suitable FortiAP profile and change the county code settings on the profile
- D. Create a new FortiAP profile and change the county code settings on the profile

Answer: C

NEW QUESTION 9

As standard best practice, which configuration should be performed before configuring FortiAPs using a FortiGate wireless controller?

- A. Create wireless LAN specific policies
- B. Preauthorize APs
- C. Create a custom AP profile
- D. Set the wireless controller country setting

Answer: D

NEW QUESTION 10

Which statement describes FortiPresence location map functionality?

- A. Provides real-time insight into user movements
- B. Provides real-time insight into user online activity
- C. Provides real-time insight into user purchase activity
- D. Provides real-time insight into user usage stats

Answer: A

NEW QUESTION 10

When using FortiPresence as a captive portal, which two types of public authentication services can be used to access guest Wi-Fi? (Choose two.)

- A. Social networks authentication
- B. Software security token authentication
- C. Short message service authentication
- D. Hardware security token authentication

Answer: AC

NEW QUESTION 15

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE6_FWF-6.4 Practice Exam Features:

- * NSE6_FWF-6.4 Questions and Answers Updated Frequently
- * NSE6_FWF-6.4 Practice Questions Verified by Expert Senior Certified Staff
- * NSE6_FWF-6.4 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * NSE6_FWF-6.4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE6_FWF-6.4 Practice Test Here](#)