NSE6_FWF-6.4 Dumps

Fortinet NSE 6 - Secure Wireless LAN 6.4

https://www.certleader.com/NSE6_FWF-6.4-dumps.html

NEW QUESTION 1
Refer to the exhibits.
Exhibit A

```
config wireless-controller wtp-profile
    edit "Main Networks - FAP-320C"
        set comment "Profile with standard networks"
        config platform
            set type 320C
        end
        set handoff-rssi 30
        set handoff-sta-thresh 30
        set ap-country GB
        config radio-1
            set band 802.11n
            set power-level 50
            set channel-utilization enable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set vap-all manual
            set vaps "Main-Wifi" "Contractors" "Guest"
"Wifi_IOT" "Wifi_POS" "Staff" "Students"
            set channel "1" "6" "11"
        end
        config radio-2
            set band 802.11ac
            set channel-bonding 40MHz
            set power-level 60
            set channel-utilization enable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set vap-all manual
            set vaps "Main-Wifi" "Contractors" "Guest"
"Wifi_IOT" "Wifi_POS" "Staff" "Students"
            set channel "36" "44" "52" "60"
        end
    next
end
```

Exhibit B

Diagnostics and Tools - Office

Office

Serial Number	FPXXXXXXXXXXXX
Base MAC Address	XX:XX:XX:XX:XX:XX
Status	✓ Online
Country/Region	GB
Uplink Interface	FortiAP management (ap)
IPv4 Address	192.168.5.98
Uptime	12m1s
Version	v6.4 build0437

Actions ▼

General
- 56% CPU Usage
- 70% Memory Usage
- 0 days Connection Uptime
- 1.0 Gbps lan1
- 0 Mbps lan2

Radio 1 - 2.4 GHz
- 31 Interfering SSIDs
- 1 Clients
- 25% Channel Utilization

Radio 2 - 5 GHz
- 0 Interfering SSIDs
- 30 Clients
- 5% Channel Utilization

Radios | Clients | Interfering SSIDs | Logs | CLI Access | Spectrum Analysis | VLAN Probe

	Radio 1 - 2.4 GHz	Radio 2 - 5 GHz
Mode	AP	AP
SSID	fortinet (Main-WiFi) fortinet2 (Contractors) fortinet3 (Guest)	fortinet (Main-WiFi) fortinet2 (Contractors) fortinet3 (Guest)
Clients	1	20
Bandwidth Tx	4.65 kbps	1.16 kbps
Bandwidth Rx	20.46 kbps	176 bps
Operating Channel	1	60
Channels		
Operating TX Power	3 dBm	21 dBm
Band	802.11n	802.11ac

Interfering SSIDs for Office (Radio 1)   ✕

⟳ Refresh | Search | 🔍

SSID ⇕	AP BSSID ⇕	Channel ⇕	Signal ⇕
Husky	aa:aa:aa:aa:aa	1	-84 dBm
Husky guest	bb:bb:bb:bb:bb	1	-84 dBm
KBANK5007	cc:cc:cc:cc:cc:cc	1	-85 dBm
mandikaylee	dd:dd:dd:dd:dd	1	-86 dBm
	ee:ee:ee:ee:ee	1	-87 dBm
HUAWEI-EMIX4f	ee:ee:ee:ee:ef	1	-88 dBm
trojan-3	ff:ff:ff:ff:ff:ff	1	-88 dBm
	fg:gg:gg:gg:gg	1	-89 dBm
	hg:gg:gg:gg:gg	1	-89 dBm

Exhibit C

```
# get wireless-controller rf-analysis FPXXXXXXXXXXXXXX

WTP: Office 0-192.168.5.98:5246

    channel    rssi-total    rf-score    overlap-ap    interfere-ap    chan-utilization
       1          100            6           13             13              63%
       2           23           10            0             22              47%
       3           15           10            0             22              15%
       4           24           10            0             22              15%
       5           51           10            0             22              41%
       6          223            1            9              9              75%
       7           52           10            0             17              47%
       8           32           10            0             17              13%
       9           27           10            0             19              10%
      10           45           10            0             19              28%
      11          177            1            8             10              65%
      12           46           10            0             10              34%
      13           45           10            2             10              70%
      14           14           10            0             10               0%
      36           16           10            2              2               0%
      44           83            7            5              5               0%
```

A wireless network has been installed in a small office building and is being used by a business to connect its wireless clients. The network is used for multiple purposes, including corporate access, guest access, and connecting point-of-sale and Io devices.
Users connecting to the guest network located in the reception area are reporting slow performance. The network administrator is reviewing the information shown in the exhibits as part of the ongoing investigation of the problem. They show the profile used for the AP and the controller RF analysis output together with a screenshot of the GUI showing a summary of the AP and its neighboring APs.
To improve performance for the users connecting to the guest network in this area, which configuration change is most likely to improve performance?

A. Increase the transmission power of the AP radios
B. Enable frequency handoff on the AP to band steer clients
C. Reduce the number of wireless networks being broadcast by the AP
D. Install another AP in the reception area to improve available bandwidth

Answer: B

NEW QUESTION 2
Which administrative access method must be enabled on a FortiGate interface to allow APs to connect and function?

A. Security Fabric
B. SSH
C. HTTPS
D. FortiTelemetry

Answer: A

NEW QUESTION 3
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 inits configured frequency band

Answer: CD

NEW QUESTION 4
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 5

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 6
What is the first discovery method used by FortiAP to locate the FortiGate wireless controller in the default configuration?

A. DHCP
B. Static
C. Broadcast

D. Multicast

Answer: B

NEW QUESTION 7
Six APs are located in a remotely based branch office and are managed by a centrally hosted FortiGate. Multiple wireless users frequently connect and roam between the APs in the remote office.
The network they connect to, is secured with WPA2-PSK. As currently configured, the WAN connection between the branch office and the centrally hosted FortiGate is unreliable.
Which configuration would enable the most reliable wireless connectivity for the remote clients?

A. Configure a tunnel mode wireless network and enable split tunneling to the local network
B. Configure a bridge mode wireless network and enable the Local standalone configuration option
C. Configure a bridge mode wireless network and enable the Local authentication configuration option
D. Install supported FortiAP and configure a bridge mode wireless network

Answer: A

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
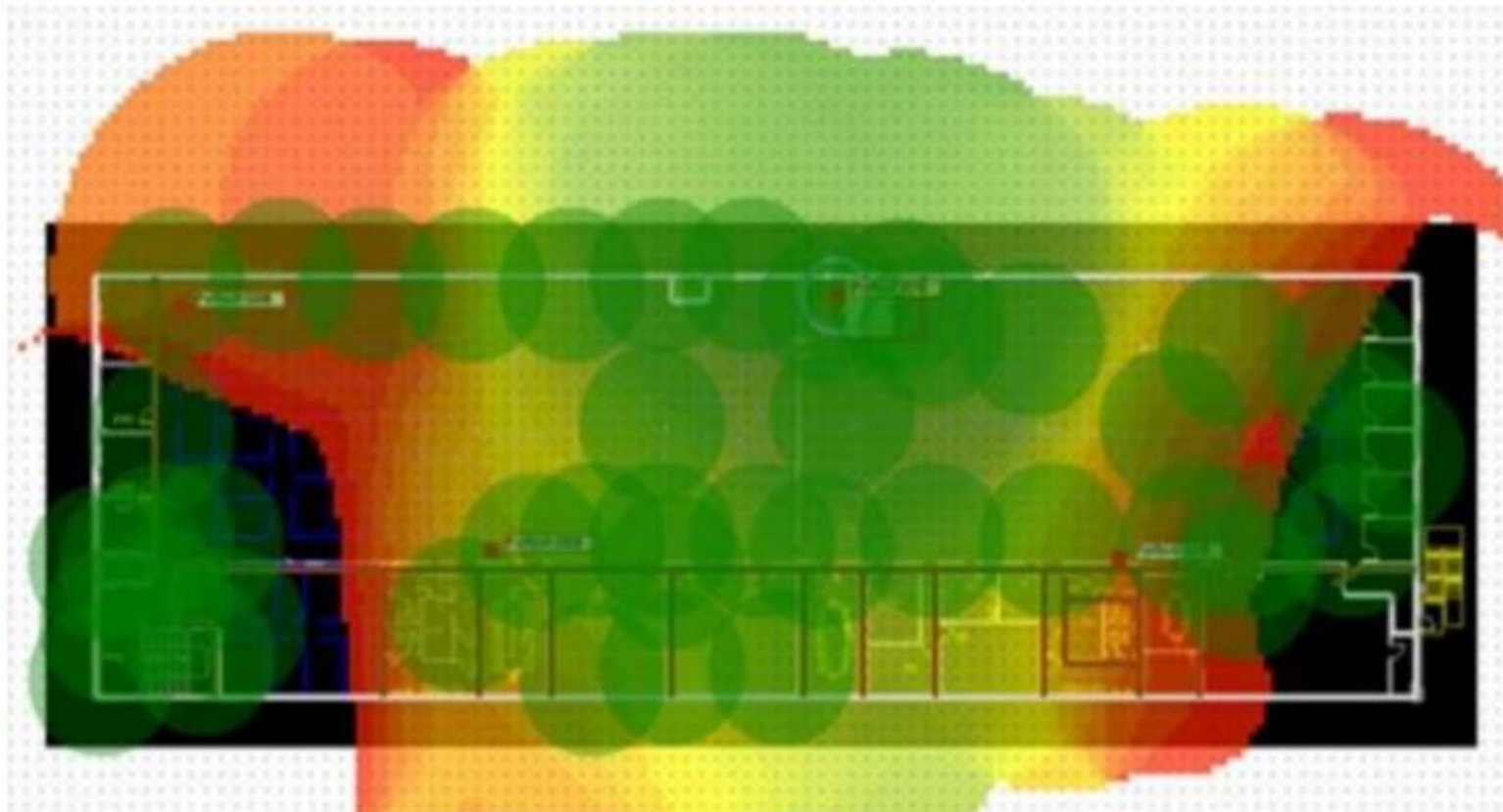
Answer: C

NEW QUESTION 9
Which two phases are part of the process to plan a wireless design project? (Choose two.)

A. Project information phase
B. Hardware selection phase
C. Site survey phase
D. Installation phase

Answer: AC

NEW QUESTION 10
Refer to the exhibit.

If the signal is set to -68 dB on the FortiPlanner site survey reading, which statement is correct regarding the coverage area?

A. Areas with the signal strength equal to -68 dB are zoomed in to provide better visibility
B. Areas with the signal strength weaker than -68 dB are cut out of the map
C. Areas with the signal strength equal or stronger than -68 dB are highlighted in multicolor
D. Areas with the signal strength weaker than -68 dB are highlighted in orange and red to indicate that no signal was propagated by the APs.

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 14
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

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your NSE6_FWF-6.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE6_FWF-6.4-dumps.html