



Fortinet

Exam Questions NSE6_FWF-6.4

Fortinet NSE 6 - Secure Wireless LAN 6.4

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
  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

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

	Radio 1 - 2.4 GHz	Radio 2 - 5 GHz
Mode	AP	AP
SSID	<ul style="list-style-type: none"> fortinet (Main-WiFi) fortinet2 (Contractors) fortinet3 (Guest) 	<ul style="list-style-type: none"> 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) x

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	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	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 IoT 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 statement is correct about security profiles on FortiAP devices?

- A. Security profiles on FortiAP devices can use FortiGate subscription to inspect the traffic
- B. Only bridge mode SSIDs can apply the security profiles
- C. Disable DTLS on FortiAP
- D. FortiGate performs inspection the wireless traffic

Answer: B

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 in its 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

When configuring Auto TX Power control on an AP radio, which two statements best describe how the radio responds? (Choose two.)

- A. When the AP detects any other wireless signal stronger than -70 dBm, it will reduce its transmission power until it reaches the minimum configured TX power limit.
- B. When the AP detects PF Interference from an unknown source such as a cordless phone with a signal stronger than -70 dBm, it will increase its transmission power until it reaches the maximum configured TX power limit.
- C. When the AP detects any wireless client signal weaker than -70 dBm, it will reduce its transmission power until it reaches the maximum configured TX power limit.
- D. When the AP detects any interference from a trusted neighboring AP stronger than -70 dBm, it will reduce its transmission power until it reaches the minimum configured TX power limit.

Answer: AC

NEW QUESTION 6

Refer to the exhibit.

Radio 2

Mode: Disabled **Access Point** Dedicated Monitor

WIDS profile: default-wids-apscan-enabled

Radio resource provision:

Band: 5 GHz 802.11ac/n/a

Channel width: **20MHz** 40MHz 80MHz

Short guard interval:

Channels:

<input checked="" type="checkbox"/> 36	<input checked="" type="checkbox"/> 40	<input checked="" type="checkbox"/> 44
<input checked="" type="checkbox"/> 48	<input checked="" type="checkbox"/> 52*	<input checked="" type="checkbox"/> 56*
<input checked="" type="checkbox"/> 60*	<input checked="" type="checkbox"/> 64*	<input checked="" type="checkbox"/> 100*
<input checked="" type="checkbox"/> 104*	<input checked="" type="checkbox"/> 108*	<input checked="" type="checkbox"/> 112*
<input checked="" type="checkbox"/> 116*	<input checked="" type="checkbox"/> 120*	<input checked="" type="checkbox"/> 124*
<input checked="" type="checkbox"/> 128*	<input checked="" type="checkbox"/> 132*	<input checked="" type="checkbox"/> 136*
<input checked="" type="checkbox"/> 140*	<input checked="" type="checkbox"/> 144*	<input checked="" type="checkbox"/> 149
<input checked="" type="checkbox"/> 153	<input checked="" type="checkbox"/> 157	<input checked="" type="checkbox"/> 161
<input checked="" type="checkbox"/> 165		

TX power control: **Auto** Manual

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 7

Refer to the exhibits.
 Exhibit A

```
config wireless-controller wtp
  edit "FPXXXXXXXXXXXXXX"
    set admin enable
    set name "Authors AP1"
    set wtp-profile "Authors"
    config radio-1
    end
    config radio-2
    end
  next
  edit "FPXXXXXXXXXXXXYYY"
    set admin enable
    set name " Authors AP2"
    set wtp-profile "Authors"
    config radio-1
    end
    config radio-2
    end
  next
  edit "FPXXXXXXXXXXXXZZZ"
    set admin enable
    set name " Authors AP3"
    set wtp-profile "Authors"
    config radio-1
    end
    config radio-2
    end
  next
end
```

Exhibit B

```
sh wireless-controller wtp-profile Authors
config wireless-controller wtp-profile
  edit "Authors"
    set comment "APs allocated to authors"
    set handoff-sta-tresh 30
    config radio-1
      set band 802.11n-5G
      set channel-bonding 40MHz
      set auto-power-level enable
      set auto-power-high 12
      set auto-power-low 1
      set vap-all tunnel
      set channel "36" "40" "44" "48" "52" "56"
      "60" "64" "100" "104" "108" "112" "116" "120" "124"
      "128" "132" "136"
    end
    config radio-2
      set band 802.11n, g-only
      set auto-power-level enable
      set auto-power-high 12
      set auto-power-low 1
      set vap-all tunnel
      set channel "1" "6" "11"
    end
  next
end
config wireless-controller vap
  edit "Authors"
    set ssid "Authors"
    set security wpa2-only-enterprise
    set radius-mac-auth enable
    set radius-mac-auth-server "Main AD"
    set local-bridging enable
    set intra-vap-privacy enable
    set schedule "always"
  next
end
```

A wireless network has been created to support a group of users in a specific area of a building. The wireless network is configured but users are unable to connect to it. The exhibits show the relevant controller configuration for the APs and the wireless network. Which two configuration changes will resolve the issue? (Choose two.)

- A. For both interfaces in the wtp-profile, configure set vaps to be "Authors"
- B. Disable intra-vap-privacy for the Authors vap-wireless network
- C. For both interfaces in the wtp-profile, configure vap-all to be manual
- D. Increase the transmission power of the AP radio interfaces

Answer: AC

NEW QUESTION 8

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 10

.....

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 FirstTry
- * 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](#)