

Exam Questions NSE6_FWF-6.4

Fortinet NSE 6 - Secure Wireless LAN 6.4

https://www.2passeasy.com/dumps/NSE6_FWF-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

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	<div><div>fortinet (Main-WiFi)</div><div>fortinet2 (Contractors)</div><div>fortinet3 (Guest)</div></div>	<div><div>fortinet (Main-WiFi)</div><div>fortinet2 (Contractors)</div><div>fortinet3 (Guest)</div></div>
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	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	rss-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 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 3

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 4

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 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

Which of the following is a requirement to generate analytic reports using on-site FortiPresence deployment?

- A. SQL services must be running
- B. Two wireless APs must be sending data
- C. DTLS encryption on wireless traffic must be turned off

D. Wireless network security must be set to open

Answer: A

NEW QUESTION 7

What type of design model does FortiPlanner use in wireless design project?

- A. Architectural model
- B. Predictive model
- C. Analytical model
- D. Integration model

Answer: B

NEW QUESTION 8

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 9

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 10

Refer to the exhibits.

Exhibit A

```
config wireless-controller wtp
  edit "FPXXXXXXXXXXXXXXX"
    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
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 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 13

Which two roles does FortiPresence analytics assist in generating presence reports? (Choose two.)

- A. Gathering details about on site visitors
- B. Predicting the number of guest users visiting on-site
- C. Comparing current data with historical records
- D. Reporting potential threats by guests on site

Answer: AC

NEW QUESTION 15

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE6_FWF-6.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE6_FWF-6.4 Product From:

https://www.2passeasy.com/dumps/NSE6_FWF-6.4/

Money Back Guarantee

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 Updatesfor 1 Year