

NSE6_FWF-6.4^{Q&As}

Fortinet NSE 6 - Secure Wireless LAN 6.4

Pass Fortinet NSE6_FWF-6.4 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse6_fwf-6-4.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

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

Correct Answer: ABE

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.

Reference: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-vlan/71683dynamicvlan-config.html>

QUESTION 2

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

Correct Answer: AD

This information along with the social network authentication logins with Facebook, Google, Instagram, LinkedIn, or FortiPresence using your WiFi.

Captive Portal configurations for social media logins and internet access. You can add and manage sites using the integrated Google maps and manoeuvre your hardware infrastructure easily.

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/e126e498-eabb11eb-97f7-00505692583a/FortiPresence-21.3-Administration_Guide.pdf

QUESTION 3

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

Correct Answer: A

Reference: <https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/788897/configuring-the-rootfortigate-and-downstream-fortigates>

QUESTION 4

Refer to the exhibits.

Exhibit A Exhibit B

```
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
```

```
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

Correct Answer: A

Best security option is WPA2-AES.

Reference: <https://www.esecurityplanet.com/trends/the-best-security-for-wireless-networks/>

QUESTION 5

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	FPXXXXXXXXXX
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
<div style="float: right;"> General 56% CPU Usage 70% Memory Usage 0 days Connection Uptime 1.0 Gbps lan1 0 Mbps lan2 </div>	
Radio 1 - 2.4 GHz <div style="display: flex; justify-content: space-between;"> 31 Interfering SSIDs 1 Clients 25% Channel Utilization </div>	
Radio 2 - 5 GHz <div style="display: flex; justify-content: space-between;"> 0 Interfering SSIDs 30 Clients 5% Channel Utilization </div>	

	Radio 1 - 2.4 GHz	Radio 2 - 5 GHz
Mode	AP	AP
SSID	AP fortinet (Main-WiFi) AP fortinet2 (Contractors) AP fortinet3 (Guest)	AP fortinet (Main-WiFi) AP fortinet2 (Contractors) AP 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 FPXXXXXXXXXXXXXXXXX
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

Correct Answer: A