Fortinet.NSE6_FWF-6.4.v2022-03-03.q10

Exam Code:	NSE6_FWF-6.4
Exam Name:	Fortinet NSE 6 - Secure Wireless LAN 6.4
Certification Provider:	Fortinet
Free Question Number:	10
Version:	v2022-03-03
# of views:	1011
# of Questions views:	100
https://www.freepdfdumps.com/Fortinet.NSE6_FWF-6.4.v2022-03-03.q10.html	

NEW QUESTION: 1
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
```

freepdfdumps.com

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
```

freepdfdumps.com

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: A (LEAVE A REPLY)

Best security option is WPA2-AES.

NEW QUESTION: 2

When deploying a wireless network that is authenticated using EAP PEAP, which two configurations are required? (Choose two.)

A. An X.509 to authenticate the authentication server

B. A WPA2 or WPA3 Enterprise wireless network

C. An X.509 certificate to authenticate the client

D. 509 certificates and work for connections that use Secure Socket Layer/Transport Level Security (SSL/TLS). Both client and server certificates have additional requirements.

E. A WPA2 or WPA3 personal wireless network

Answer: (SHOW ANSWER)

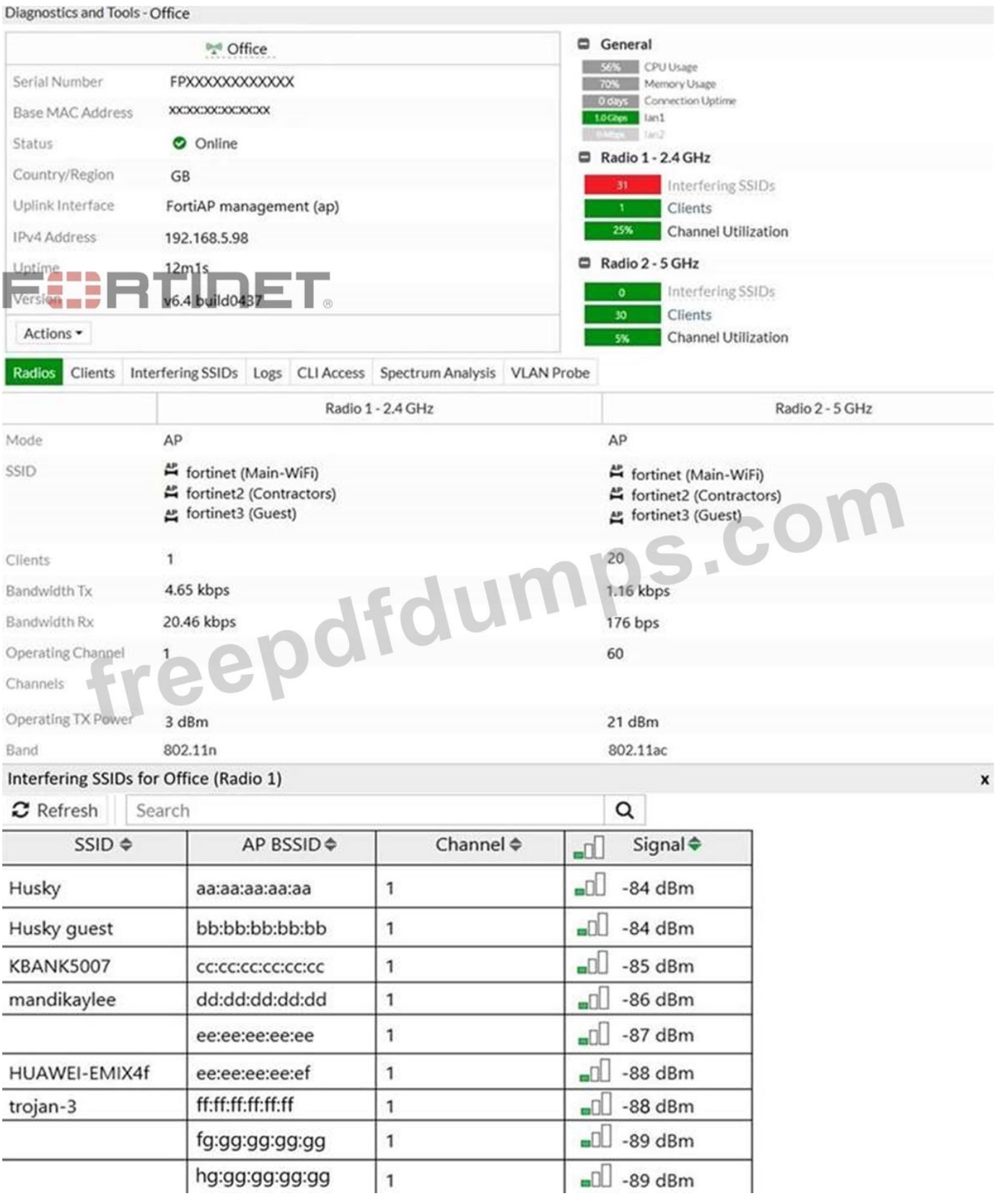
NEW QUESTION: 3

Refer to the exhibits.

Exhibit A

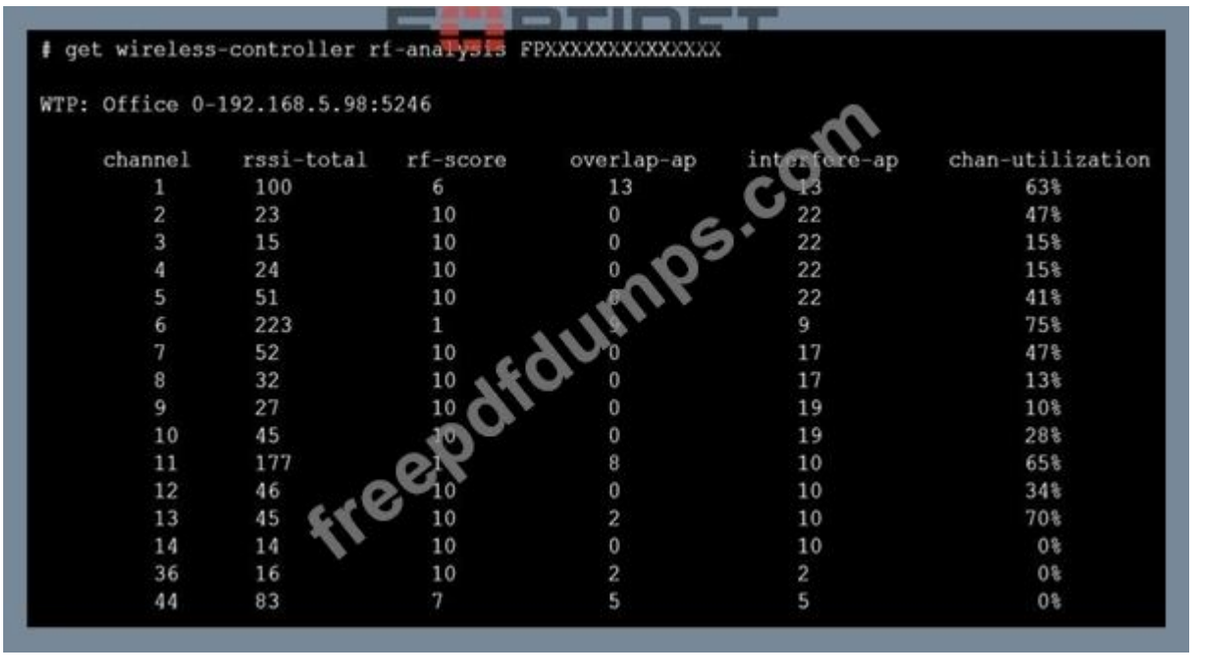
freepdfdumps.com

Exhibit B



FORTINET
freepdfdumps.com

Exhibit C



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

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            1              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%
```

freepdfdumps.com

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. Enable frequency handoff on the AP to band steer clients

B. Install another AP in the reception area to improve available bandwidth

C. Increase the transmission power of the AP radios

D. Reduce the number of wireless networks being broadcast by the AP

Answer: (SHOW ANSWER)

NEW QUESTION: 4

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: B (LEAVE A REPLY)

NEW QUESTION: 5

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: (SHOW ANSWER)
To enable rogue AP scanning

NEW QUESTION: 6
When enabling security fabric on the FortiGate interface to manage FortiAPs, which two types of communication channels are established between FortiGate and FortiAPs? (Choose two.)
A. Control channels
B. Security channels
C. FortLink channels
D. Data channels
Answer: (SHOW ANSWER)
The control channel for managing traffic, which is always encrypted by DTLS. I The data channel for carrying client data packets.

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. Install supported FortiAP and configure a bridge mode wireless network
C. Configure a bridge mode wireless network and enable the Local standalone configuration option
D. Configure a bridge mode wireless network and enable the Local authentication configuration option
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
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: C,D (LEAVE A REPLY)
Reference:
https://www.automation.com/en-us/articles/2015-2/wireless-device-network-planning-and-design

NEW QUESTION: 9
Which statement is correct about security profiles on FortiAP devices?
A. Only bridge mode SSIDs can apply the security profiles
B. Security profiles on FortiAP devices can use FortiGate subscription to inspect the traffic
C. Disable DTLS on FortiAP
D. FortiGate performs inspection the wireless traffic
Answer: A (LEAVE A REPLY)

NEW QUESTION: 10
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: B,D (LEAVE A REPLY)
In the SSID choose WPA2-Enterprise authentication.
WSSO is RADIUS-based authentication that passes the user's user group memberships to the FortiGate.

Valid NSE6_FWF-6.4 Dumps shared by Actual4test.com for Helping Passing NSE6_FWF-6.4 Exam! Actual4test.com now offer the **newest NSE6_FWF-6.4 exam dumps**, the Actual4test.com NSE6_FWF-6.4 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NSE6_FWF-6.4 dumps with Test Engine here: https://www.actual4test.com/NSE6_FWF-6.4_examcollection.html (**37** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)