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

A. An X.509 certificate to authenticate the client
B. An X.509 to authenticate the authentication server
C. A WPA2 or WPA3 personal wireless network
D. A WPA2 or WPA3 Enterprise wireless network

Answer: BD

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 that -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 that -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 that -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 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 7
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 8
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 9
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 10
Which factor is the best indicator of wireless client connection quality?

A. Downstream link rate, the connection rate for the AP to the client
B. The receive signal strength (RSS) of the client at the AP
C. Upstream link rate, the connection rate for the client to the AP
D. The channel utilization of the channel the client is using

Answer: C

NEW QUESTION 10
Refer to the exhibit.

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

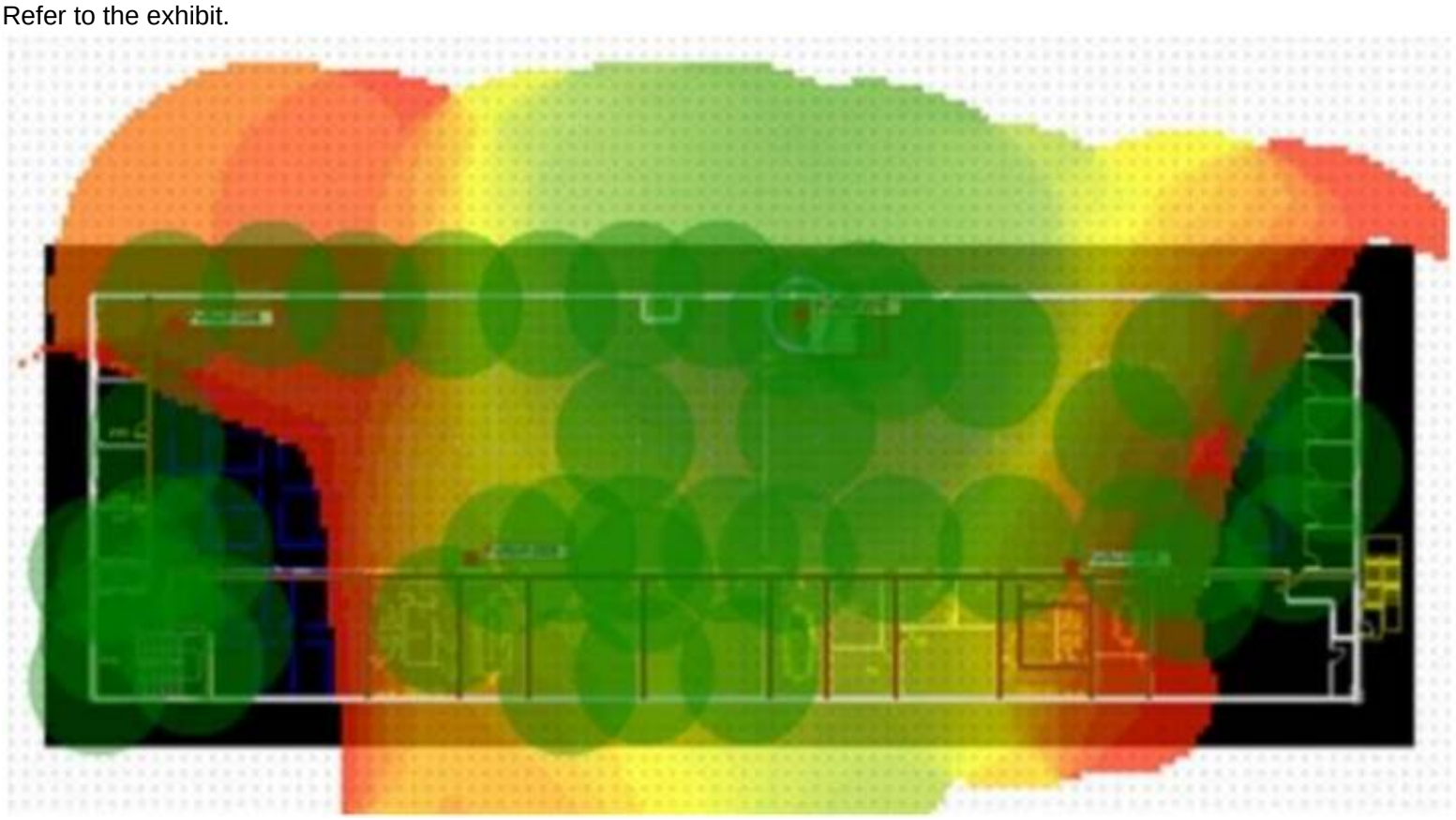
Answer: D

NEW QUESTION 12
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 14
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 18
Refer to the exhibits.
Exhibit A

```
config wireless-controller wtp
    edit "FPXXXXXXXXXXXXX"
        set admin enable
        set name "Authors AP1"
        set wtp-profile "Authors"
        config radio-1
        end
        config radio-2
        end
    next
    edit "FPXXXXXXXXXXXYYY"
        set admin enable
        set name " Authors AP2"
        set wtp-profile "Authors"
        config radio-1
        end
        config radio-2
        end
    next
    edit "FPXXXXXXXXXXXZZZ"
        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 23
.....

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