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.pass4itsure.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

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

Correct Answer: B

SSI, or "Received Signal Strength Indicator," is a measurement of how well your device can hear a signal from an access point or router. It\\'s a value that is useful for determining if you have enough signal to get a good wireless connection. Reference: https://www.metageek.com/training/resources/understanding-rssi.html

QUESTION 2

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

Correct Answer: AB

X.509 certificates and work for connections that use Secure Socket Layer/Transport Level Security (SSL/TLS). Both client and server certificates have additional requirements. Reference: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-manage-cert-requirements

QUESTION 3

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

Correct Answer: AD

The control channel for managing traffic, which is always encrypted by DTLS. l The data channel for carrying client data packets.

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ac61f4d3-ce67-11e9-8977-00505692583a/FortiWiFi_and_FortiAP-6.2-Cookbook.pdf

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

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/71683-dynamicvlan-config.html

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.

Correct Answer: AB

To enable rogue AP scanning Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/723e20ad-5098-11e9-94bf-00505692583a/FortiWiFi_and_FortiAP-6.2.0-Configuration_Guide.pdf

QUESTION 6

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

Correct Answer: CD

Reference: https://www.sciencedirect.com/topics/computer-science/wireless-site-survey https://www.automation.com/en-us/articles/2015-2/wireless-device-network-planning-and-design

QUESTION 7

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

Correct Answer: D

This geographical data analysis provides real-time insights into user behavior.

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/05d8bae1-5f3c-11e9-81a4-005056 92583a/FortiPresence-v2.0.1-getting-started.pdf

QUESTION 8

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	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	📶 fortinet (Main-WiFi) 📶 fortinet2 (Contractors) 📶 fortinet3 (Guest)	📶 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

↻ 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: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: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 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            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 Io? 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

QUESTION 9

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

Correct Answer: AB

QUESTION 10

Which statement is correct about security profiles on FortiAP devices?

A. Security profiles can only be applied to unencrypted wireless traffic.

B. Security profiles can only be applied via firewall policies on the FortiGate.

C. Security profiles are only supported on Bridge-mode SSIDs.

D. Security profiles on FortiAP devices can use FortiGate subscription to inspect the traffic.

Correct Answer: D

Security profiles on FortiAP devices can use FortiGate subscription to inspect the traffic, such as antivirus, web filtering, application control, and IPS. This feature is called local bridging and it allows the FortiAP to forward traffic to the FortiGate for security inspection before sending it to the destination network. This reduces the bandwidth consumption and latency of tunnel mode SSIDs. References: Secure Wireless LAN Course Description, page 9; [FortiOS 6.4.0 Handbook - Wireless Controller], page 46.

Latest NSE6_FWF-6.4 Dumps

NSE6_FWF-6.4 VCE Dumps

NSE6_FWF-6.4 Study Guide