Fortinet FCP_FWF_AD-7.4 NSE 5 Practice Questions

Shared by Mathis on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A wireless station has reported several connection issues with FortiAP that have not been resolved using standard troubleshooting tools As a wireless network administrator you are planning to perform additional advanced-level troubleshooting Which two steps must you take to analyze and troubleshoot the issue? (Choose two)

Options:

A- Create and assign a new FortiAP profile detected for troubleshooting
B- Capture the wireless station traffic in the air
C- Review event logs reporting wireless station activities
D- Collect low-level information on FortiAP power management

Answer:

B

Question 2

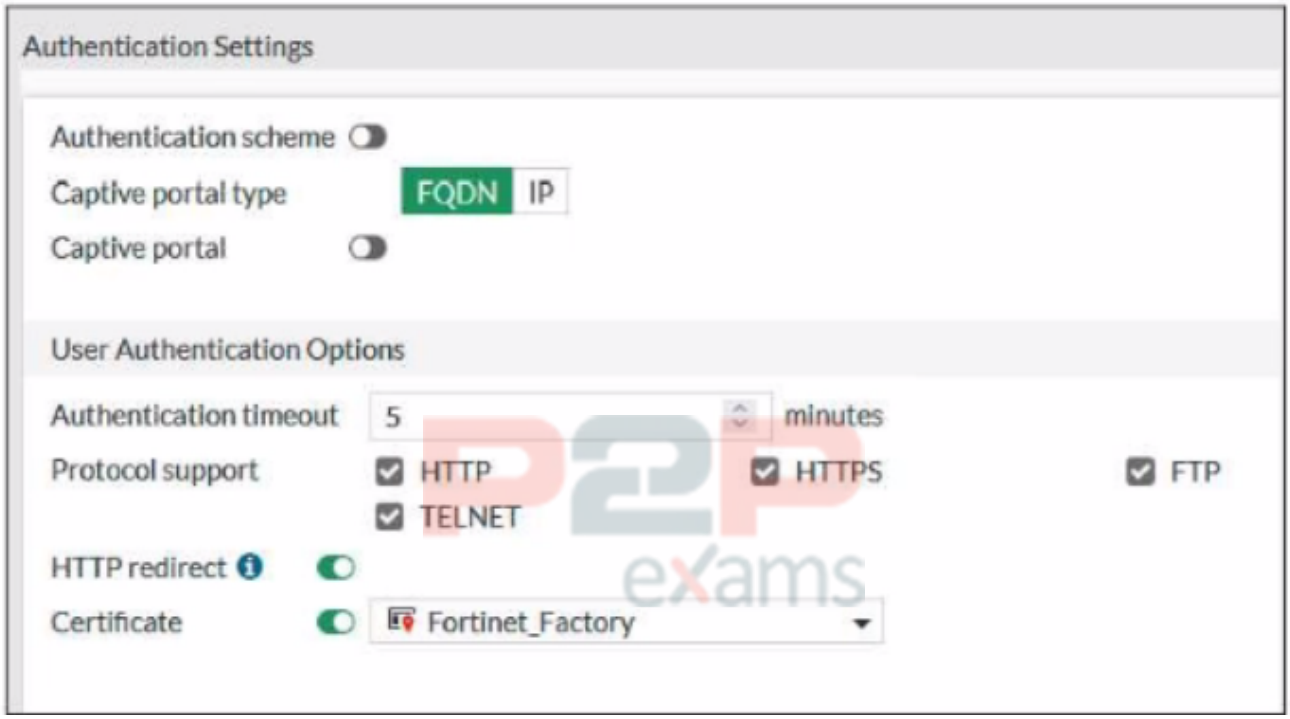
Question Type: MultipleChoice

Refer to the exhibits.

Captive portal POST parameters

```
https://10.0.1.150/guests/login/?login&post=https://auth.trainingad.training.lab:1003/f
gtauth&magic=000a038293d1f411&usermac=b8:27:eb:d8:50:02&apmac=70:4c:a5:9d:0d:28&apip=10
.10.100.2&userip=10.0.3.1&ssid=Guest03&apname=FP231FTF20011555&bssid=70:4c:a5:9d:0d:30
```

Captive portal authentication settings



FortiGate is pushing the POST parameters shown in the exhibit to the external captive portal server The wireless client redirection fails because certificate validation occurred while loading the web page

The wireless client browser uses the FortiGate self-signed certificate to access secured web pages The SSID on FortiGate has the captive portal setting

What could cause the certification validation error on the wireless client?

Options:

A- The FortiGate IP address in the POST parameters is using a numerical IP address
B- The external server address is not the FQDN address
C- The used credential is not embedded in the captive portal parameters
D- The captive portal setting in the authentication setting is set to use FQDN as the captive portal type

Answer:

A

Question 3

Question Type: MultipleChoice

When enabling a Security Fabric connection on a FortiGate interface to manage FortiAP devices, which two types of CAPWAP communication channels are established between FortiGate and the FortiAP devices'? (Select two)

Options:

A- Control channels
B- Data channels
C- Security channels
D- Fortlink channels

Answer:

A, B

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

WiFi events

Date/Time	Action	Message	Security Mode	SSID	Channel
2024/05/02 18:11:26	client-authentication	Client 5a:29:94:87:f7:b8 authenticated.	WPA3 Enterprise Transition	CORP_DATA	1
2024/05/02 18:11:26	WPA-4/4-key-msg	AP received 4/4 message of 4-way handshake from client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	1
2024/05/02 18:11:26	WPA-3/4-key-msg	AP sent 3/4 message of 4-way handshake to client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	1
2024/05/02 18:11:26	WPA-2/4-key-msg	AP received 2/4 message of 4-way handshake from client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	1
2024/05/02 18:11:26	WPA-1/4-key-msg	AP sent 1/4 message of 4-way handshake to client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	1
2024/05/02 18:11:26	client-association-failure	Client 5a:29:94:87:f7:b8 RADIUS authentication success	WPA3 Enterprise Transition	CORP_DATA	1
2024/05/02 18:11:23	assoc-resp	AP sent association response frame to client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	1
2024/05/02 18:11:23	layer3-roaming-rehome	AP received association request frame from client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	1
2024/05/02 18:11:23	auth-req-WPA3	AP received WPA3(non-SAE) authentication request frame from client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	1
2024/05/02 18:11:23	auth-resp-WPA3	AP sent WPA3(non-SAE) authentication response frame to client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	1
2024/05/02 18:11:23	auth-req-WPA3	AP received WPA3(non-SAE) authentication request frame from client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	1
2024/05/02 18:10:55	deauth	AP sent deauthentication frame to client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	100
2024/05/02 18:10:55	deauth	AP sent deauthentication frame to client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	100
2024/05/02 18:10:54	client-deauthentication	Client 5a:29:94:87:f7:b8 de-authenticated.	WPA3 Enterprise Transition	CORP_DATA	100
2024/05/02 18:10:54	client-association-failure	Client 5a:29:94:87:f7:b8 RADIUS authentication failure	WPA3 Enterprise Transition	CORP_DATA	100
2024/05/02 18:10:54	assoc-resp	AP sent association response frame to client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	100
2024/05/02 18:10:54	layer3-roaming-rehome	AP received association request frame from client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	100
2024/05/02 18:10:54	auth-resp-WPA3	AP sent WPA3(non-SAE) authentication response frame to client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	100
2024/05/02 18:10:54	auth-req-WPA3	AP received WPA3(non-SAE) authentication request frame from client 5a:29:94:87:f7:b8	WPA3 Enterprise Transition	CORP_DATA	100

The wireless station with MAC address 5a:29:94:87:f7:b8 has made multiple attempts to connect to the CORP.DATA SSID Despite client-association-failure event logs the wireless station connects on the final attempt

Why did the wireless station fail to connect initially?

Options:

A- The wireless station connected to SSID but failed RADIUS authentication
B- The wireless controller unauthenticated the wireless station to prevent evil twin attacks
C- The wireless station was incompatible with the 5 GHz radio band.
D- The wireless station used invalid credentials on the failed attempt

Answer:

A

Question 5

Question Type: MultipleChoice

Which two statements are correct about FortiAP and rogue APs? (Choose two.)

Options:

A- FortiAP offers automatic suppression of rogue APs when broadcasting SSIDs
B- FortiAP scans rogue APs in the background while broadcasting SSIDs
C- FortiAP detects rogue APs on dedicated monitoring radios
D- FortiAP suppresses detected rogue APs manually

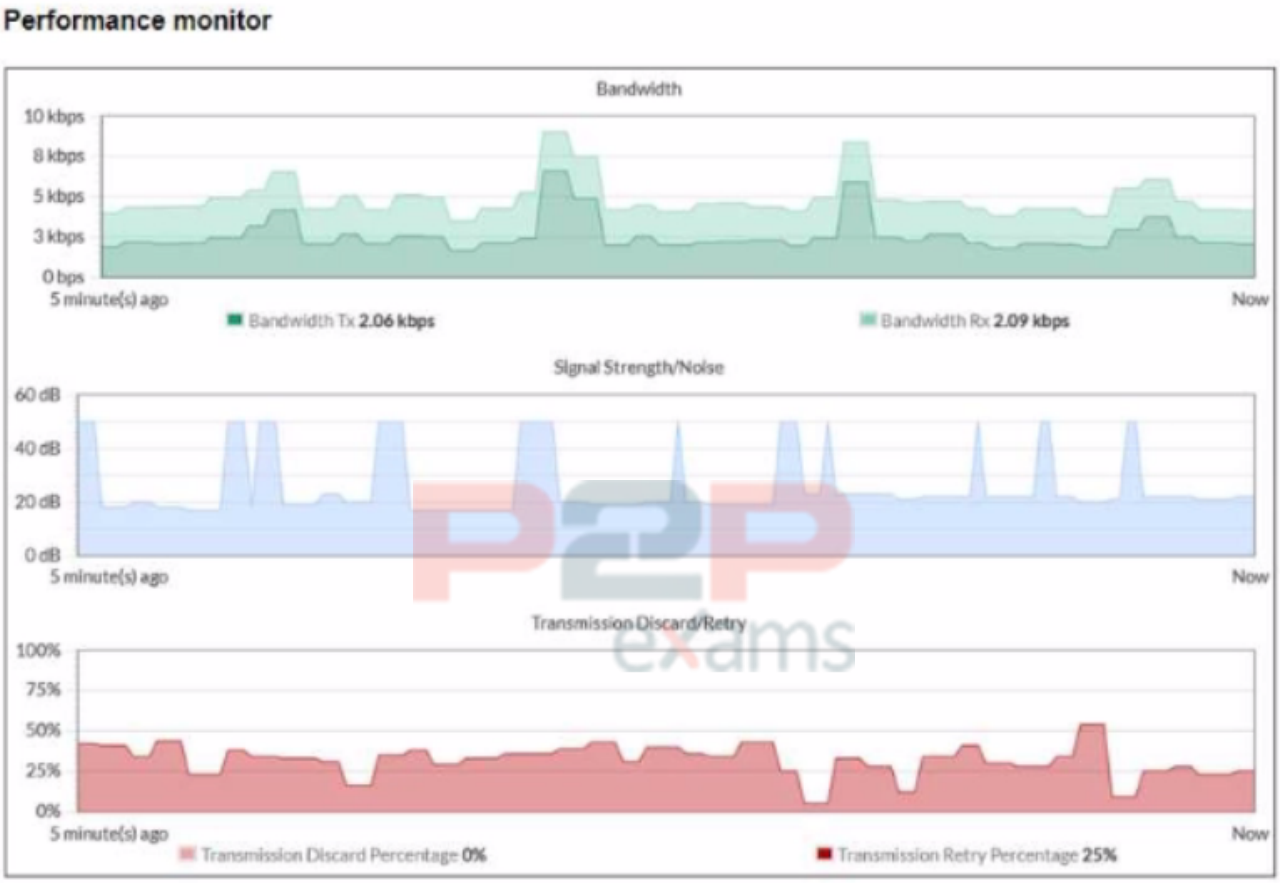
Answer:

B, C

Question 6

Question Type: MultipleChoice

Exhibit.



Refer to the exhibit of a wireless client performance monitor Which performance metric is abnormal for this wireless client?

Options:

A- The wireless client has been experiencing high background noise within the last 5 minutes
B- The wireless client has been dropping half of the packets transmitted within the last 5 minutes.
C- The wireless client has been transmitting traffic with all performance metrics within the normal levels
D- The wireless client has been switching between available wireless bands within the last 5 minutes

Answer:

B

Question 7

Question Type: MultipleChoice

How can you find the upstream and downstream link rates of a wireless client connected to a

FortiAP?

Options:

A- On the FortiGate GUI using the WiFi Client monitor
B- On the FortiAP CLI using the cw_diag ksta command
C- On the FortiGate CL! using the diagnose wireless-controller wlac -d sta command
D- On the FortiAP CLI using the cw_diag -d sea command

Answer:

B

Question 8

Question Type: MultipleChoice

A FortiAP device is connected directly to a FortiGate interlace. What discovery method will be used to provision the FortiAP device?

Options:

A- FortiGate discovers the FortiAP IP address from DHCP option 138.
B- FortiGate discovers the FortiAP through the received broadcast packets.
C- FortiAP discovers FortiGate by reviewing the vendor class value.
D- FortiAP discovers FortiGate by connecting to FortiLAN Cloud to verify its management license.

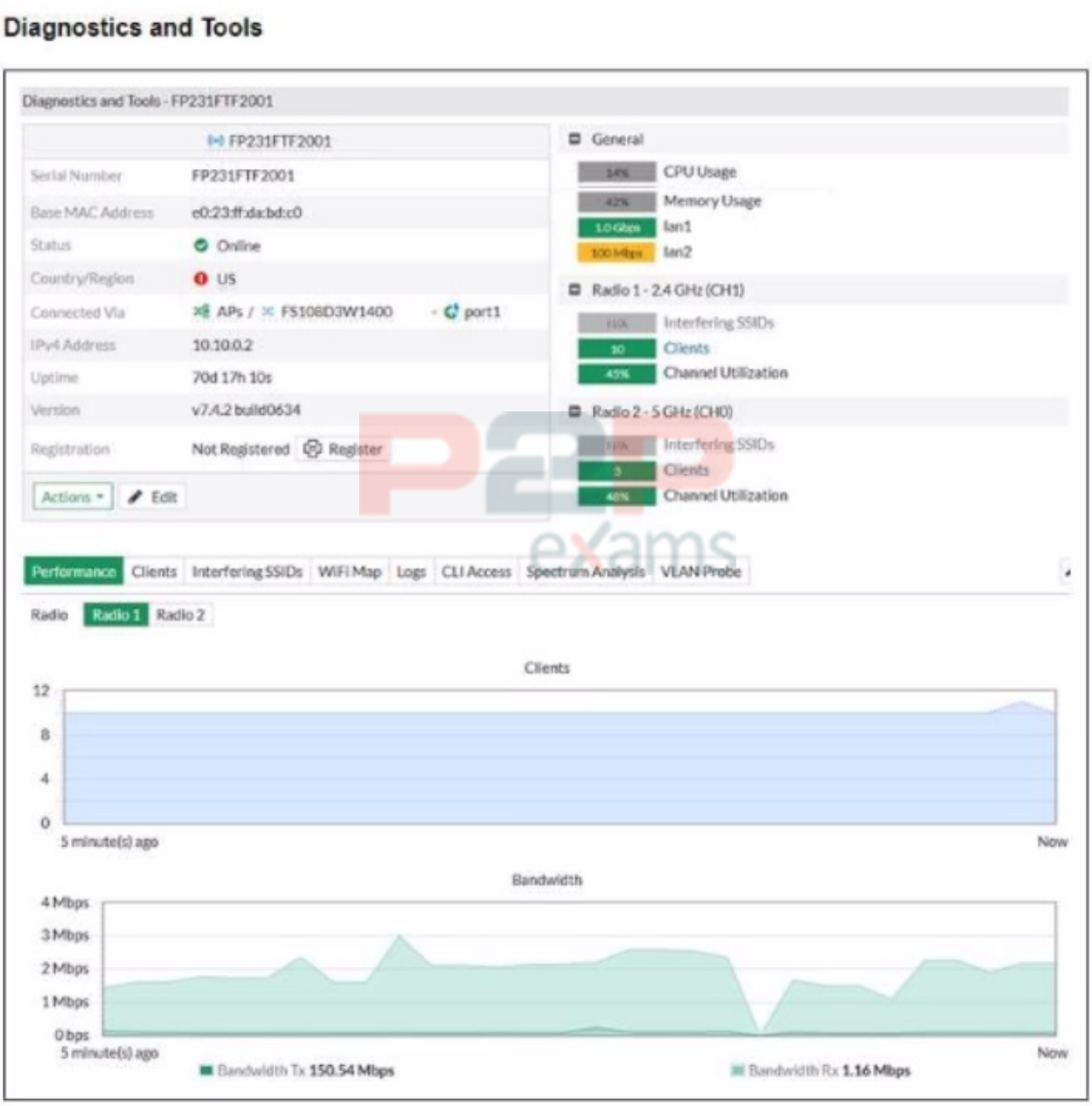
Answer:

B

Question 9

Question Type: MultipleChoice

Exhibit.



Refer to the exhibit of FortiAP performance diagnostics

The wireless users are having issues with wireless network speed while connecting to the only FortiAP device As an administrator you accessed the FortiAP diagnostics and tools to explore performance graphs

The label shows that the transmission bandwidth should be at least 150 Mbps. however the bandwidth graph shows that the transmission only hit 3 Mbps maximum within the last 5 minutes

What can you observe from this?

Options:

A- Resources on FortiAP are overloaded which limits speed rates for all users

B- Label values are historical and provide average bandwidth
C- FortiAP is dual band and is transmitting data faster with a higher frequency band
D- Bandwidth is shared with other SSID signals broadcasting for nearby AP devices

Answer:

C

Question 10

Question Type: MultipleChoice

A wireless station has reported several connection issues with FortiAP that have not been resolved using standard troubleshooting tools As a wireless network administrator you are planning to perform additional advanced-level troubleshooting Which two steps must you take to analyze and troubleshoot the issue? (Select two)

Options:

A- Create and assign a new FortiAP profile detected for troubleshooting
B- Capture the wireless station traffic in the air
C- Review event logs reporting wireless station activities
D- Collect low-level information on FortiAP power management

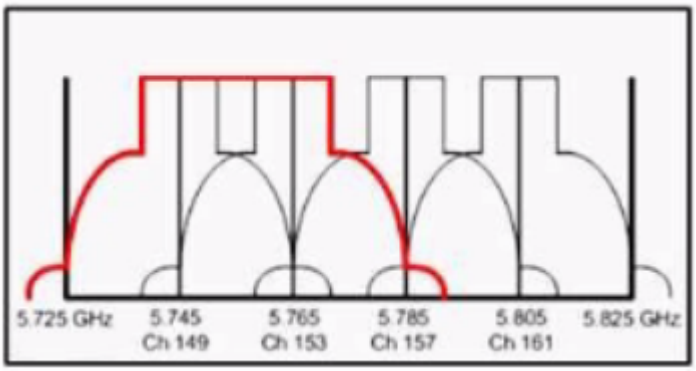
Answer:

B

Question 11

Question Type: MultipleChoice

Refer to the exhibit.



What does the red line represent?

Options:

A- Practical channel bonding to increase high throughput
B- A pool of channels for the wireless radio to broadcast the wireless signal.
C- The range of channels used to allocate available airtime while transmitting data
D- The total length of the wireless signal wavelength

Answer:

A

Question 12

Question Type: MultipleChoice

Refer to the exhibit.

Access Point	SSIDs	Channel	Clients	OS Version	FortiAP Profile	Connected Via
Online 2						
FP231FT	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs R3 N/A	R1 1 R2 140 R3 N/A	11	v7.4.2 build0634	FAP231F	APs
FP23JFT	R1 N/A R2 N/A R3 N/A	R1 N/A R2 N/A R3 N/A	0	v7.4.2 build0634	FAP23JF	APs

An administrator authorizes two FortiAP devices connected to this wireless controller However, one FortiAP is not able to broadcast the SSIDs. What must the administrator do to fix the issue?

Options:

A- Enable the radios on the FAP23JF FortiAP profile.

B- Replace the FortiAP device model to match the other device
C- Disable the override setting on the FortiAP that is preventing it from broadcasting SSIDs
D- Assign the FAP231F FortiAP profile to the problematic FortiAP device

Answer:

A

P2P exams