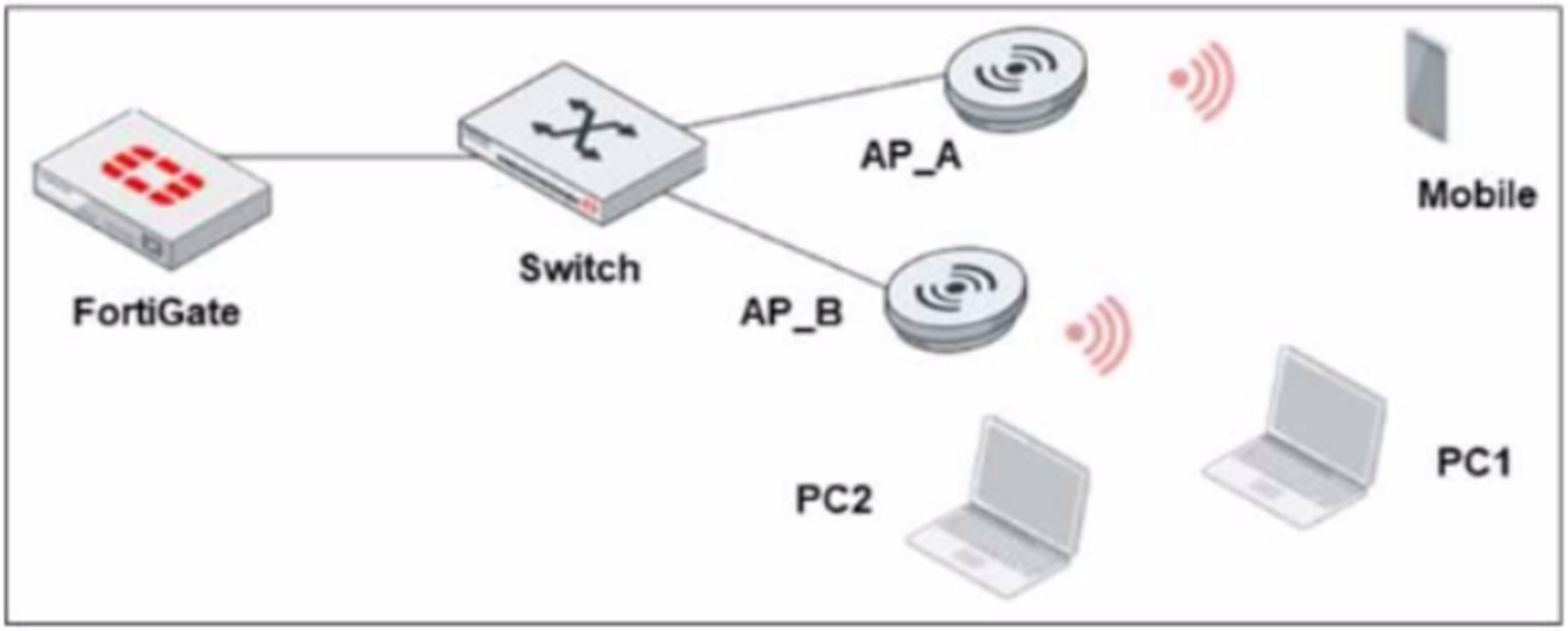
Exam Questions FCP_FWF_AD-7.4

FCP - Secure Wireless LAN 7.4 Administrator

https://www.2passeasy.com/dumps/FCP_FWF_AD-7.4/

NEW QUESTION 1
Refer to the exhibit.



A new security policy is made by the IT department to prevent direct communication between wireless stations There is one SSID configured in bridge mode
Which statement is correct as a plan of action to update the wireless network configuration?

A. Create unique SSIDs for each FortiAP device
B. Add an upstream layer 3 device on each FortiAP device
C. Block intra-SSID traffic on the wireless network
D. Drop all local traffic in the wireless network

Answer: C

Explanation:
Scenario:
The IT department wants to prevent direct communication between wireless stations.
There is one SSID configured in bridge mode (all clients on the same SSID/VLAN, directly bridging to the wired network).
Correct Action:
Block intra-SSID traffic (sometimes called ??client isolation?? or ??intra-SSID privacy??).
This feature prevents wireless clients connected to the same SSID from communicating directly with each other at Layer 2.
Each station can reach the network but cannot reach other wireless clients on the same SSID.
This is the industry-standard method to achieve the stated security goal in a wireless environment, especially in bridge mode.
Why Other Options Are Incorrect:
* A. Create unique SSIDs for each FortiAP device
Impractical and unnecessary for user isolation; users on the same SSID but different APs can still be isolated with intra-SSID blocking.
* B. Add an upstream layer 3 device on each FortiAP device
Overkill and not required; this does not directly solve intra-SSID traffic.
* D. Drop all local traffic in the wireless network
Too broad; you only want to prevent client-to-client communication, not all local traffic (such as traffic to the gateway).
Summary:
Block intra-SSID traffic is the intended and correct configuration to prevent wireless stations from communicating directly while sharing the same SSID in bridge mode.

NEW QUESTION 2
You plan to deploy a wireless network at various remote sites with no on-site IT available. The remote sites must have access points to broadcast the wireless networks You can manage the access points using any Fortinet control and management option
Which two items must you consider in addition to deploying the wireless network and enforcing Fortinet UTM on all wireless traffic? (Choose two.)

A. To install the access points designed to provide Fortinet UTM services
B. To power the access points with a UIM capable FortSwitch device
C. To deploy the SSIDs in bridge mode bridged to the access points subnet
D. To manage the access points by FortiLAN Cloud and create a tunnel between access points

Answer: AD

Explanation:
For remote sites with no on-site IT, you should:
A: Use APs that support Fortinet UTM (i.e., FortiAPs that can tunnel traffic back to a FortiGate for UTM enforcement).
D: Use cloud-based management (FortiLAN Cloud) and configure tunnel SSIDs so all traffic from the AP is sent back for security inspection at a central FortiGate.
B refers to PoE power but isn??t essential if APs can be powered in another way.
C (bridge mode to local subnet) would not allow centralized UTM enforcement unless local FortiGate is present.

NEW QUESTION 3
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?

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

Explanation:
The logs show repeated client-association-failure events followed by RADIUS authentication failure messages for client
This means the station successfully associated at Layer 2 but failed at the RADIUS authentication step X/EAP), typically due to invalid credentials or a misconfiguration on the RADIUS server.
Eventually, the log shows a successful authentication, indicating the credentials or RADIUS issue was resolved on a later attempt.

NEW QUESTION 4
You must design a wireless network to accommodate wireless stations to access local resources and the internet The access level of these stations will vary based on the type of device and users
Which design must you use to provide wireless access that will fulfill these requirements?

A. Create user groups to assign wireless stations once connected to an SSID
B. Create multiple SSIDs for each level of network access
C. Create an SSID and enable dynamic wireless VLAN
D. Create an SSID and enable integrated wireless NAC

Answer: C

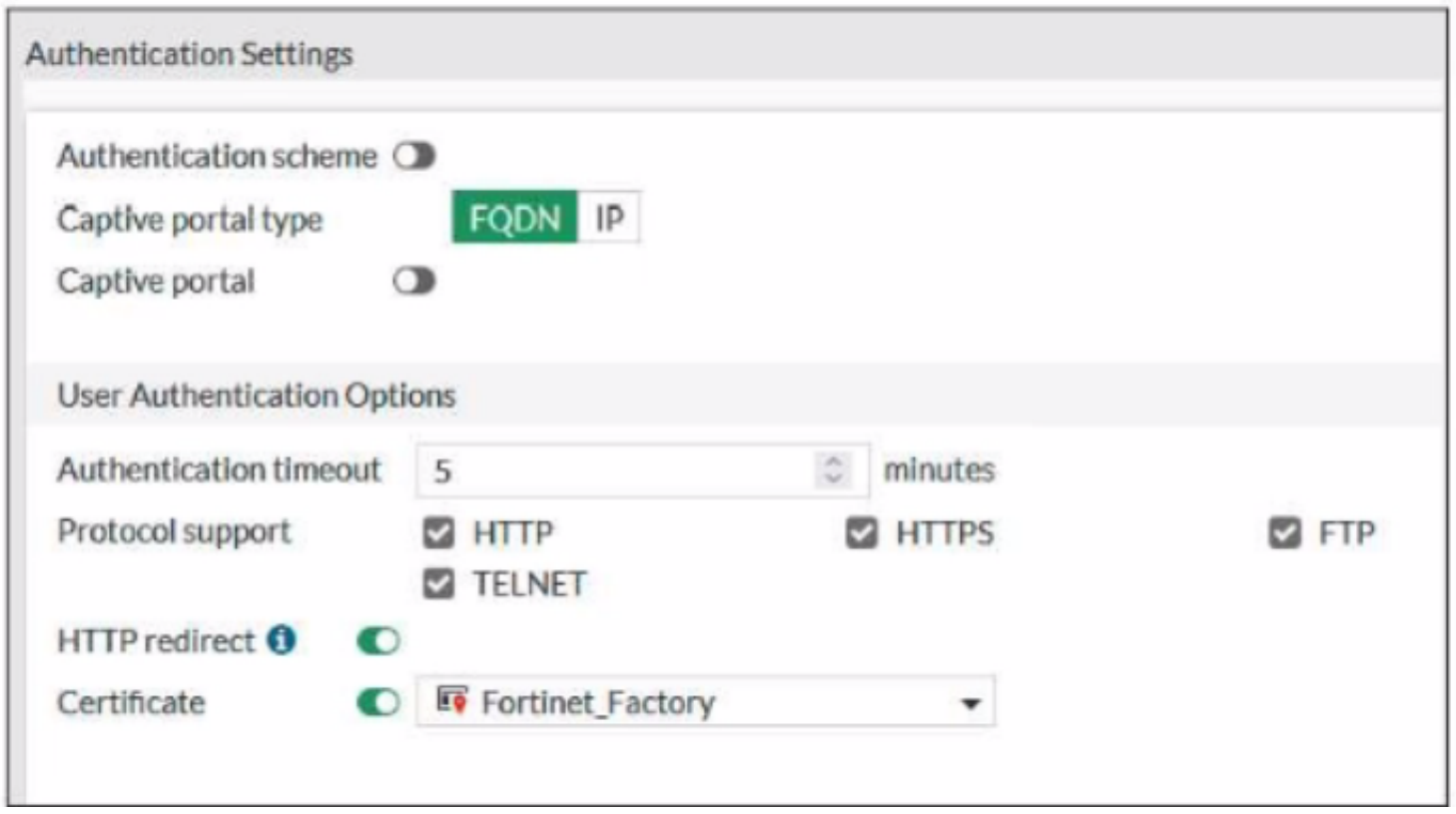
Explanation:
When you need different access levels for various users and device types but want to keep the SSID structure simple, dynamic VLAN assignment is the best practice.
With dynamic VLANs, all clients connect to the same SSID. The RADIUS server (via 802.1X authentication or MAC authentication) assigns each user or device to a specific VLAN based on attributes (like user group, device type, etc.).
This design:
Reduces SSID sprawl.
Allows flexible, scalable, and policy-driven access.
Simplifies management and enhances security.
The other options are either less scalable (multiple SSIDs) or do not provide the required dynamic access control (user groups or NAC alone without VLAN assignment).

NEW QUESTION 5
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?

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: D

Explanation:
Scenario Analysis:
The wireless client is redirected to a captive portal for authentication.
The authentication settings (see second exhibit) show:
Captive portal type: FQDNis selected.
Certificate:Fortinet_Factory(the default self-signed certificate).
The browser is reporting acertificate validation errorwhen the redirection to the captive portal occurs.
Certificate Validation and Captive Portals:
When FQDN is used for captive portal redirection, the browser expects the SSLcertificate to be valid for the FQDN (e.g., ??captive.company.com??).
If the certificate isself-signedor doesnot match the FQDN(common when using the Fortinet factory default certificate), the browser will trigger a certificate error.
This is a common issue when FQDN-based portals are used without apublicly trusted certificate matching the FQDN.
Option Analysis:
* A. The FortiGate IP address in the POST parameters is using a numerical IP address
Not relevant; the browser validates the page being loaded, not the POST parameters.
* B. The external server address is not the FQDN address
In this case, the external captive portal URLisusing FQDN, as set in the authentication setting.
* C. The used credential is not embedded in the captive portal parameters
Credential handling is not related to certificate errors; it would result in login/authentication failures, not browser SSL warnings.
* D. The captive portal setting in the authentication setting is set to use FQDN as the captive portal type
Correct.When FQDN is used, the SSL certificate presented must be trusted and match the FQDN. The factory certificate will not match (it is not publicly trusted), so clients will see a validation error.
Summary:
Certificate validation fails because the captive portal is accessed via FQDN, but the FortiGate presents its self-signed factory certificate, which does not match the FQDN or is not trusted by browsers.

NEW QUESTION 6
An IT department must provide wireless security to employees connected over remote hortiAP devices who must access corporate resources at the mam office
Which action must the IT department take to enforce security policies for all wireless stations accessing corporate resources across all remote locations?

A. Configure VPN tunnels to transport secured data between the main office and branch offices
B. Deploy further onsite IT personnel to these remote sites to enforce security inspection
C. Transfer local resources from corporate data centers to cloud services to offer access to remote users
D. Implement a teleworker topology to split traffic for further security inspection

Answer: D

Explanation:
The scenario involves employees connecting via remote FortiAP (FAP) devices, with a requirement to enforce corporate security policies for all wireless stations at branch/remote sites.
Teleworker topology(also called remote AP, or split-tunnel mode) is designed exactly for this:
FortiAP at remote sites connects to the main office FortiGate via a secure tunnel (CAPWAP over VPN or DTLS).
Traffic destined for corporate resources is tunneled back to the main officefor full security inspection and policy enforcement.
Local internet-bound traffic can be split off locally (split-tunnel) or tunneled back as well (full-tunnel), based on policy.
This ensures all employee wireless sessions accessing corporate resources are subject to central security policies, without requiring local IT staff.
Option A(VPN tunnels) ispartof the teleworker topology but doesn't by itself ensure wireless security enforcement or policy application for wireless stations—teleworker/split-tunnel is more precise.
Option Bis impractical and unnecessary.
Option Cmoves resources to the cloud, but this does not ensure security enforcement for wireless clients over remote links.
Summary:Teleworker topology on FortiAP allows secure, policy-enforced connectivity from remote sites back to HQ for all wireless stations.

NEW QUESTION 7
Refer to the exhibit.

Which statement is correct about channels 52 through 144 in the 5 GHz band?

A. The channels will be scanned by the wireless intrusion detection system (WIDS)
B. The channels cannot be used because of regulatory channel restrictions
C. The channels can be used only when Radio Resource Provisioning is enabled
D. The channels are subject to dynamic frequency selection (DPS) regulations

Answer: D

Explanation:
Channels 52 through 144 in the 5 GHz band (shown as UNII-2, UNII-2-Extended, and some adjacent channels) are marked in regulatory domains as DFS (Dynamic Frequency Selection) channels.
DFS channels must be monitored for radar activity (such as weather radar). If radar is detected, the AP must switch channels to avoid interference.
These channels can be used, but only if the AP supports DFS and performs the necessary checks before use.
WIDS can scan these channels but that??s not the defining characteristic.
Regulatory restrictions (B) apply only if DFS is not supported, which is rare on modern equipment.
Radio Resource Provisioning (C) is unrelated to DFS usage.

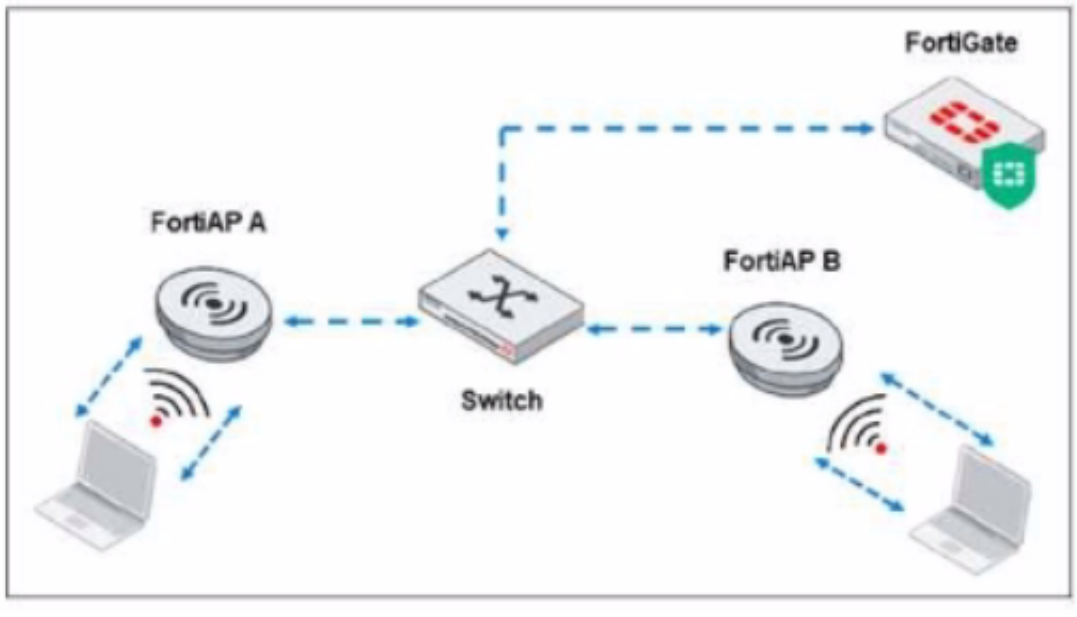
NEW QUESTION 8
What protection does WPA3 wireless encryption provide over WPA2 for securing wireless networks?

A. WPA3 uses 128-bit session key size
B. WPA3 enforces only enterprise security mode
C. WPA3 addresses the KRACK vulnerability
D. WPA3 prevents legacy and deprecated wireless protocols from being used

Answer: C

Explanation:
WPA3 introduces improvements over WPA2, most notably replacing the PSK (Pre-Shared Key) handshake with the Simultaneous Authentication of Equals (SAE) handshake.
The SAE handshake is resistant to key reinstallation attacks (KRACK) that affected WPA2.
WPA3 also improves security in open networks but does not force enterprise-only mode or universally block all legacy protocols, and 128-bit key size alone isn??t unique to WPA3.

NEW QUESTION 9
Refer to the exhibit.



Which traffic is crucial between the FortiAP devices and FortiGate to support AP configuration updates and management services?

A. Control traffic
B. Layer 2 traffic
C. Data traffic
D. License management traffic

Answer: A

Explanation:
Control traffic (CAPWAP control) is crucial for AP configuration, updates, monitoring, and management between FortiAP and FortiGate.
Data traffic carries user/client data, but management/configuration relies on control traffic.

NEW QUESTION 10
Which two threats on wireless networks are detected by WIDS? (Choose two.)
A. Brute-force dictionary attacks
B. Unauthorized wireless connection
C. Rogue access points
D. WPA2 authentication vulnerabilities

A.

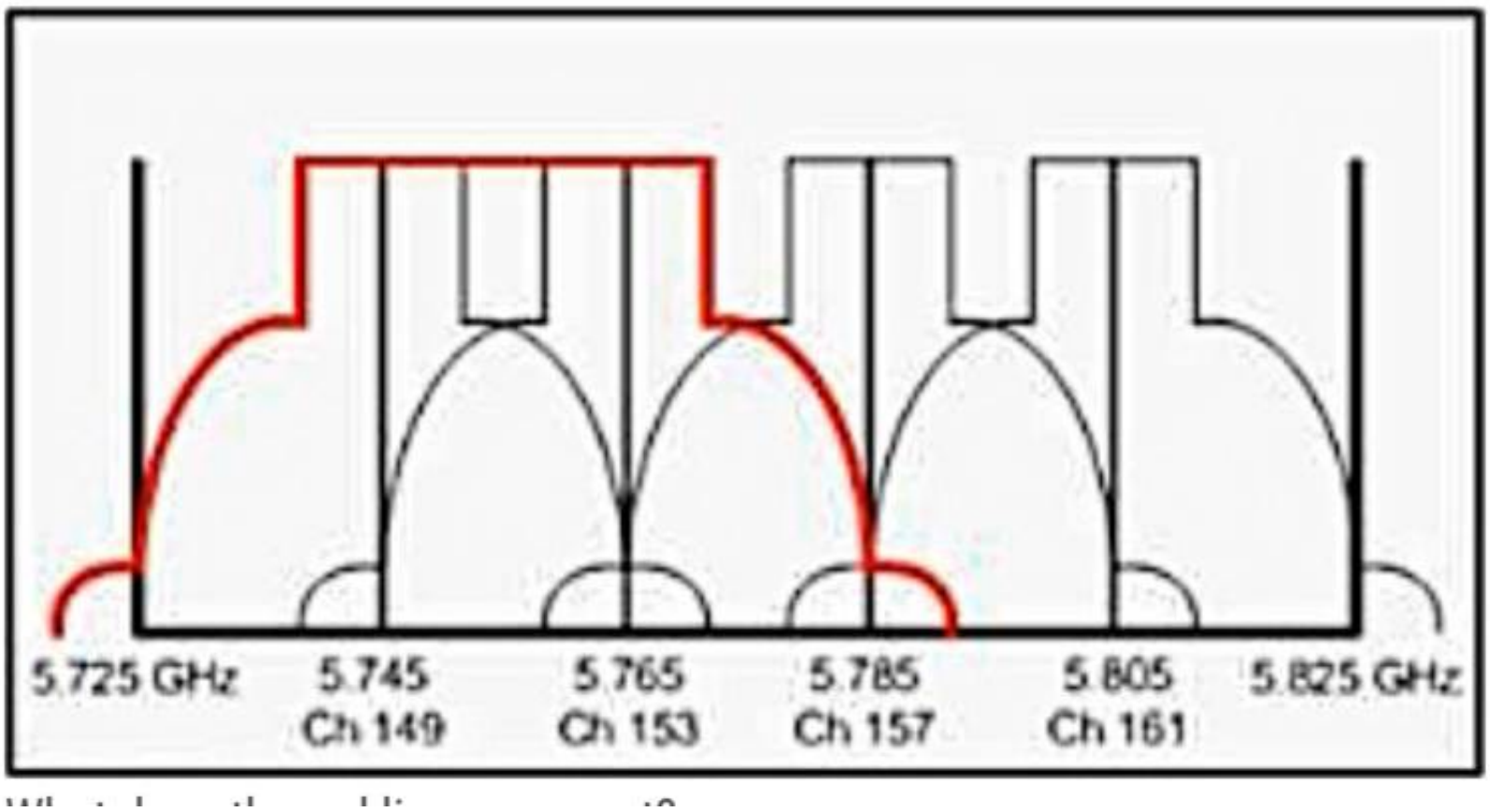
Answer: BC

NEW QUESTION 10
Which action does a wireless client or the access point take when the wireless client moves away from an associated AP until the signal drops?

A. The wireless client disconnects and connects to a different, available AP
B. The associated AP marks the wireless client as disconnected and must not reconnect
C. The associated AP sends an alert message to the wireless client about the signal drop
D. The wireless client increases its signal power to continue connecting to the same AP

Answer: A

NEW QUESTION 13
Refer to the exhibit.



What does the red line represent?

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

Explanation:
Exhibit Analysis:
The diagram shows a section of the 5 GHz Wi-Fi band, with several adjacent channels: 149, 153, 157, 161.
The red line outlines a wider frequency range covering multiple adjacent channels (149, 153, 157).
What this means:
In Wi-Fi (especially 802.11ac/ax), ??channel bonding?? means combining adjacent 20 MHz channels into a wider channel (40, 80, or even 160 MHz).
The red line indicates the frequency range that would be used if an 80 MHz channel (covering channels 149, 153, 157, 161) is formed by bonding the narrower channels together.
This increases throughput because a wider channel allows more data to be transmitted at once.
Option Review:
A. Practical channel bonding to increase high throughput

Correct. The red line represents the spectrum occupied when several 20 MHz channels are bonded into a single, wider channel to increase data rates.
* B. A pool of channels for the wireless radio to broadcast the wireless signal.
Incorrect. A pool would be all available channels, not the bonded range.
* C. The range of channels used to allocate available airtime while transmitting data
Incorrect. This is about frequency, not time.
* D. The total length of the wireless signal wavelength
Incorrect. The line indicates frequency spectrum, not wavelength length.
Summary:
The red line shows how multiple adjacent 20 MHz channels are bonded together (in this case, most likely into an 80 MHz channel), a practical method to increase wireless throughput in modern Wi-Fi networks.

NEW QUESTION 14
Which wireless monitoring metric is required to optimize a wireless network?

A. FortiAP running firmware status
B. Amount of event togs generated
C. Users count on the network
D. Wireless channel utilization

Answer: D

Explanation:
Channel utilization directly measures how much airtime is consumed by wireless transmissions (including data, management, and interference).
Monitoring channel utilization helps optimize the network by:
Identifying congestion or over-utilized channels.
Allowing channel re-planning and SSID optimization.
The other options (AP firmware, event logs, user count) are helpful, but only channel utilization gives actionable insight for radio resource optimization.

NEW QUESTION 17
What is the relationship between wireless channels and data transmission?

A. The wider the channel the more data it can carry
B. Data is transmitted over only one wireless channel at a time
C. The more wireless channels, the more power consumption is required
D. A wireless channel is allocated to transmit data unidirectionally

Answer: A

Explanation:
Wireless channels have a defined bandwidth (e.g., 20 MHz, 40 MHz, 80 MHz).
Wider channels can carry more data simultaneously, as there??s more spectral space for transmission.
Modern Wi-Fi standards (802.11n/ac/ax) use channel bonding to increase throughput by widening channels.
The other options are not correct:
Data can be transmitted across multiple bonded channels.
More channels do not necessarily mean higher power use.
Channels are used bidirectionally.

NEW QUESTION 19
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FWF_AD-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FWF_AD-7.4 Product From:

https://www.2passeasy.com/dumps/FCP_FWF_AD-7.4/

Money Back Guarantee

FCP_FWF_AD-7.4 Practice Exam Features:

* FCP_FWF_AD-7.4 Questions and Answers Updated Frequently

* FCP_FWF_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCP_FWF_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCP_FWF_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year