Fortinet

Exam Questions FCP_FWF_AD-7.4

FCP - Secure Wireless LAN 7.4 Administrator

NEW QUESTION 1
Which benefit does 802.1X authentication offer when securing a wireless network?

A. Authentication and authorization m enterprise networks
B. Allows administrators to gain elevated privilege to access resources
C. Makes wireless access at home protected and secured
D. Simplifies public Wi-Fi hotspots for guest access

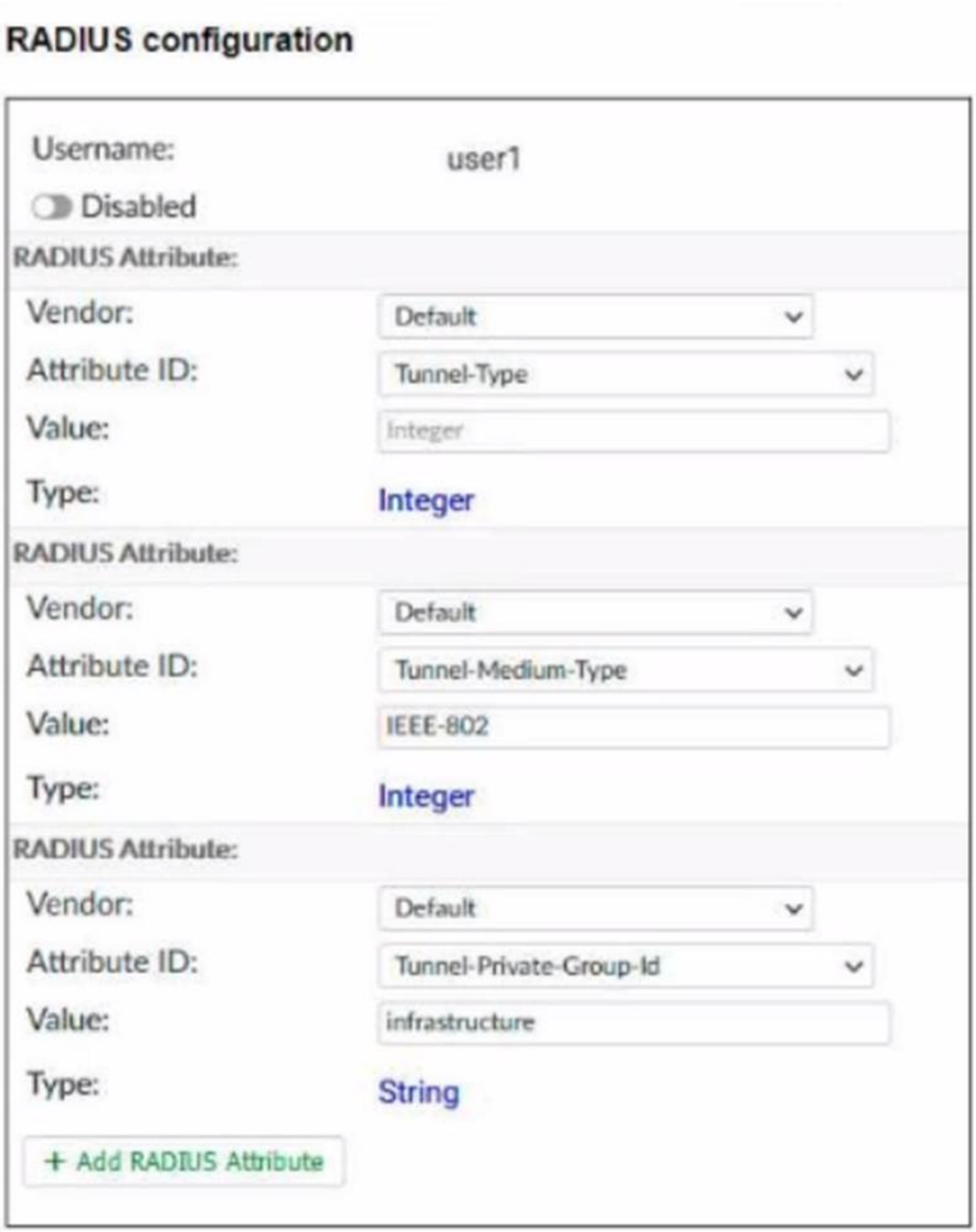
Answer: A

Explanation:
* 802.1 X is the standard for port-based network access control, widely used in enterprise Wi-Fi to:
Authenticate users and devices before granting access to the network.
Authorize network access (optionally placing users into specific VLANs).
It is not for home Wi-Fi (C), does not provide admin privilege (B), and is more complex than open guest Wi- Fi (D).

NEW QUESTION 2
Refer to the exhibit.

DHCP server settings

```
config system dhcp server
    edit 1
        set dns-service default
        set default-gateway 10.0.10.254
        set netmask 255.255.255.0
        set interface "WLAN01"
        config ip-range
            edit 1
                set start-ip 10.0.10.2
                set end-ip 10.0.10.100
            next
        end
    next
end
```



User1 is part of the infrastructure department and connects to the ONBOARD wireless network using the credentials uteri. However, the dynamic VLAN assignment is not working
Which configuration step must you take to fix this issue?

A. Disable the DHCP server on ONBOARD to allow VLAN assignment.
B. Add user1 in one of the VLAN names
C. Update user1 RADIUS attributes to include a VLAN ID attribute ID
D. Create a new VLAN name infrastructure' with a VLAN ID associated with it

Answer: C

Explanation:
Analysis of the Exhibits and Scenario:
The DHCP server configuration is correct for dynamic assignment within a specified IP range for the interface ??WLAN01??.
The RADIUS configuration for user1 includes:
Tunnel-Type (should be set to VLAN, but value is missing)
Tunnel-Medium-Type (set to IEEE-802, which is correct for Ethernet/WiFi) Tunnel-Private-Group-Id (set to ??infrastructure?? as a string)
The problem described: Dynamic VLAN assignment is not working for user1.
How Dynamic VLAN Assignment Works in 802.1X/EAP (with FortiGate/FortiAP):
When a user authenticates, the RADIUS server returns attributes specifying the VLAN that should be assigned.
The critical attributes are:
Tunnel-Type (must be set to value ??VLAN??, which is integer 13) Tunnel-Medium-Type (must be ??IEEE-802??, integer 6)

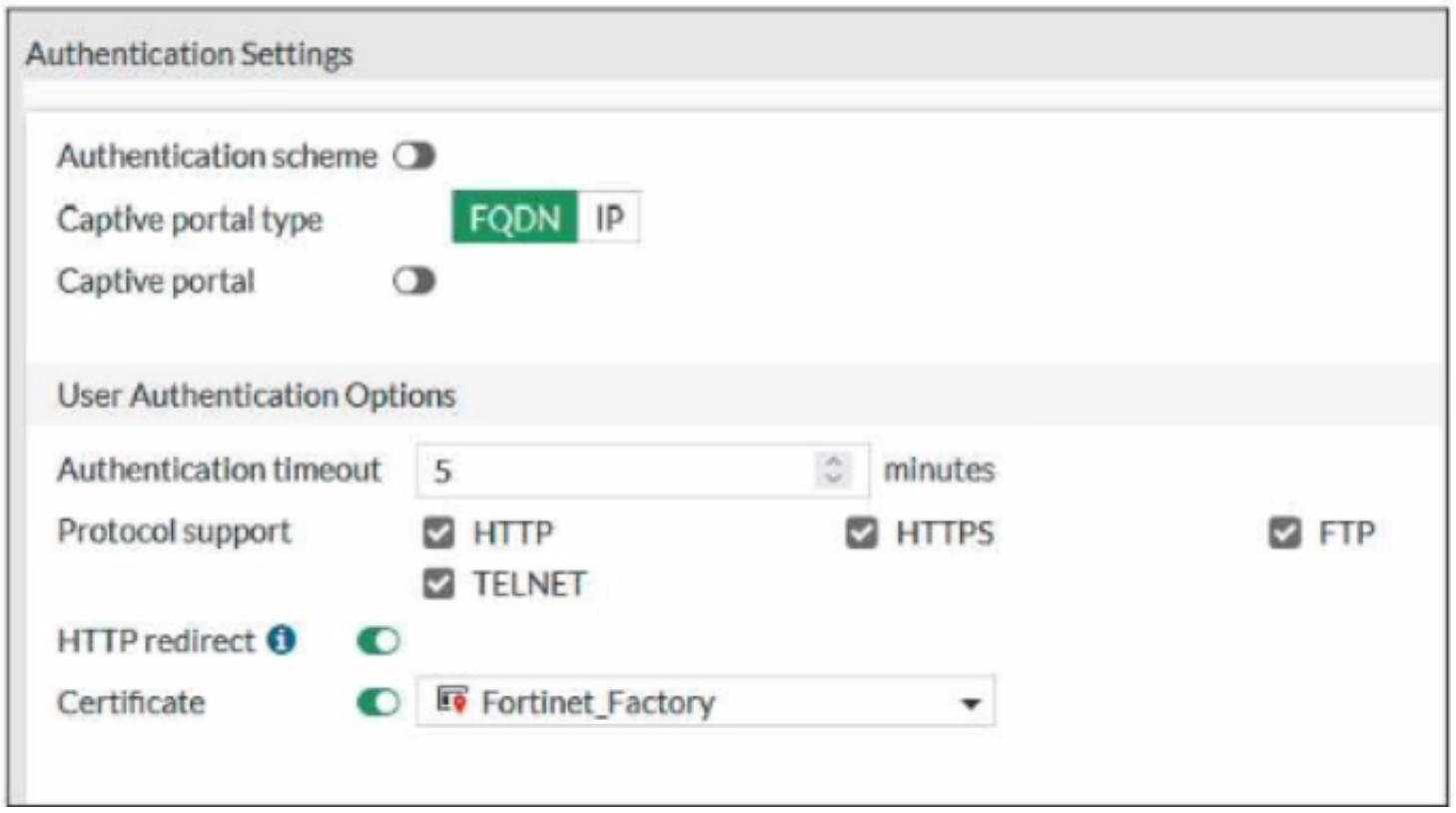
Tunnel-Private-Group-Id (can be the VLAN name or VLAN ID, depending on your configuration) Problem in the Exhibit:
The Tunnel-Type value is missing! It must be set to 13 (for VLAN).
The Tunnel-Medium-Type and Tunnel-Private-Group-Id are correctly set. Corrective Action:
Update user1??s RADIUS attributes so that Tunnel-Type is set to the correct value for VLAN (integer 13).
Without this, FortiGate/FortiAP will not know to interpret the returned VLAN name or ID for dynamic assignment.
Review of Options:
Disable the DHCP server on ONBOARD to allow VLAN assignment. Irrelevant; DHCP server presence does not affect dynamic VLAN assignment. Add user1 in one of the VLAN names
This is not how dynamic VLAN assignment works. The RADIUS response must include the correct VLAN assignment.
Update user1 RADIUS attributes to include a VLAN ID attribute ID
Correct. You must set Tunnel-Type (13) and possibly provide the VLAN ID in Tunnel-Private-Group-Id. Create a new VLAN name infrastructure' with a VLAN ID associated with it
Not the root cause; you must first ensure the correct attributes are present in the RADIUS response. Summary:
The missing ??Tunnel-Type?? attribute value is the reason dynamic VLAN assignment is not working. The correct configuration requires setting Tunnel-Type = 13 (VLAN) for user1 in the RADIUS server.

NEW QUESTION 3
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 4
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.

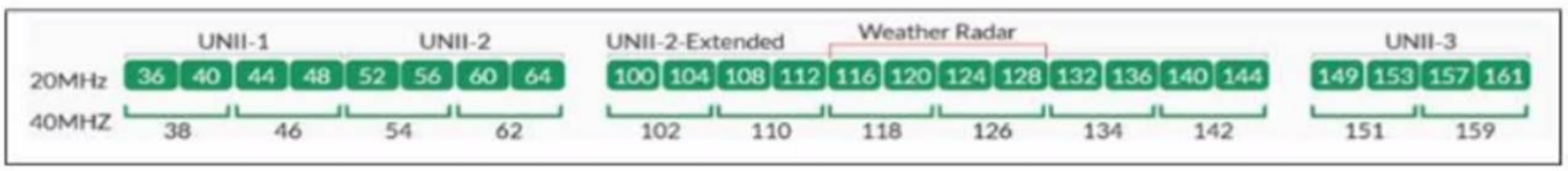
NEW QUESTION 5
A FortiAP device is connected directly to a FortiGate interlace. What discovery method will be used to provision the FortiAP device?

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

Explanation:
When a FortiAP is directly cabled to a FortiGate interface, it sends out a broadcast CAPWAP discovery packet.
The FortiGate listens for these on its interfaces and then discovers/provisions the FortiAP automatically.

NEW QUESTION 6
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 7
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 8
Which two statements are correct about FortiAP and rogue APs? (Choose two.)

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: BC

Explanation:
FortiAP and Rogue AP Detection: Background Scanning:
FortiAPs can perform background scanning for rogue APs while actively servicing clients (broadcasting SSIDs). This means they periodically switch from client service to scan the air for unauthorized APs.
This enables detection of threats without a dedicated radio, using periodic scans on service radios. Manual Suppression:
Suppression of rogue APs (for example, sending de-auth frames to clients of a rogue) must be triggered manually by an administrator from the FortiGate/FortiAP interface.
Automatic Suppression:
FortiAPs do NOT offer automatic suppression of rogue APs by default. Suppression is an explicit administrative action.
Dedicated Monitoring Radios:
Some APs (higher-end models) may have dedicated radios, but this is not the case for all FortiAPs; background scanning is the standard.
Option Breakdown:
* A. FortiAP offers automatic suppression of rogue APs when broadcasting SSIDs Incorrect. Suppression is manual.
* B. FortiAP scans rogue APs in the background while broadcasting SSIDs Correct. Background scanning is supported.
* C. FortiAP detects rogue APs on dedicated monitoring radios
Incorrect for most deployments. Dedicated monitoring radios are available only in some models.
* D. FortiAP suppresses detected rogue APs manually Correct. Manual suppression is available via the management interface.

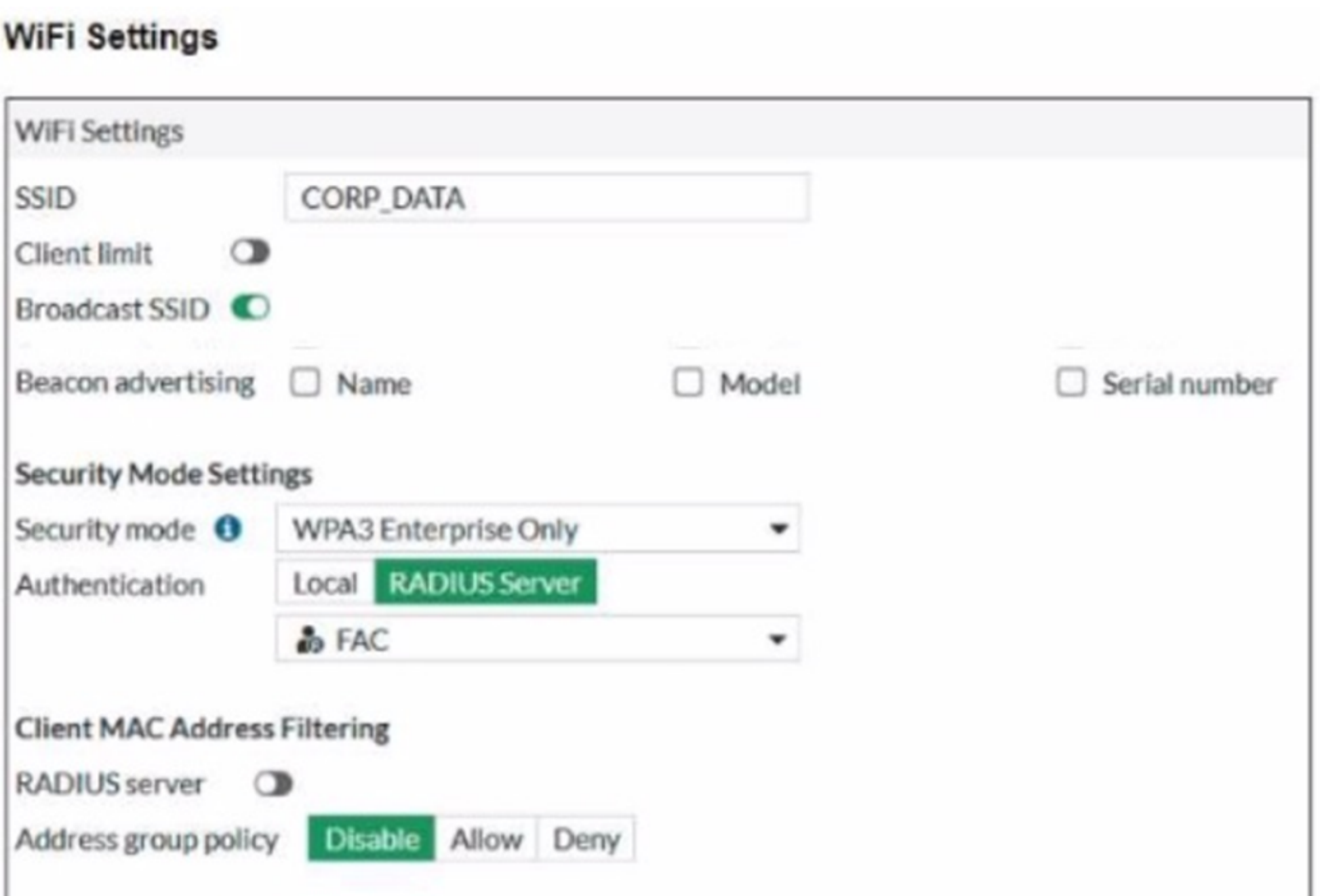
NEW QUESTION 9
Which security solution can you implement in the Security Fabric to identify and prevent threats?

A. Integrated wireless network access
B. Endpoint detection and response
C. Compromised wireless client quarantine
D. Indicator of attack system

Answer: B

Explanation:
WPA3 improves security over WPA2 by, among other things:
Using robust key establishment (SAE/Dragonfly), which is not vulnerable to KRACK (Key Reinstallation Attack).
WPA3 does not enforce only enterprise mode, nor does it universally prevent all legacy protocols, nor is 128- bit key size unique to WPA3.

NEW QUESTION 10
Refer to the exhibit.



FortiGate sends logs to FortiAnalyzer using the default settings to report security events for all wireless stations as part of the Security Fabric configuration
Which security action will FortiGate take when it detects a compromised wireless station in the CORP_DATASSlD?
A. CORP_DATA is in NAC mode and onboards compromised stations for a period until malicious activity stops
B. FortiGate disassociates compromised stations and prevents them from connecting again
C. FortiAnalyzer generates security reports to inform security operations to further Investigate the compromised stations
D. FortiAP devices broadcasting CORP_DATA wireless network place compromised stations in quarantine

A.

Answer: A

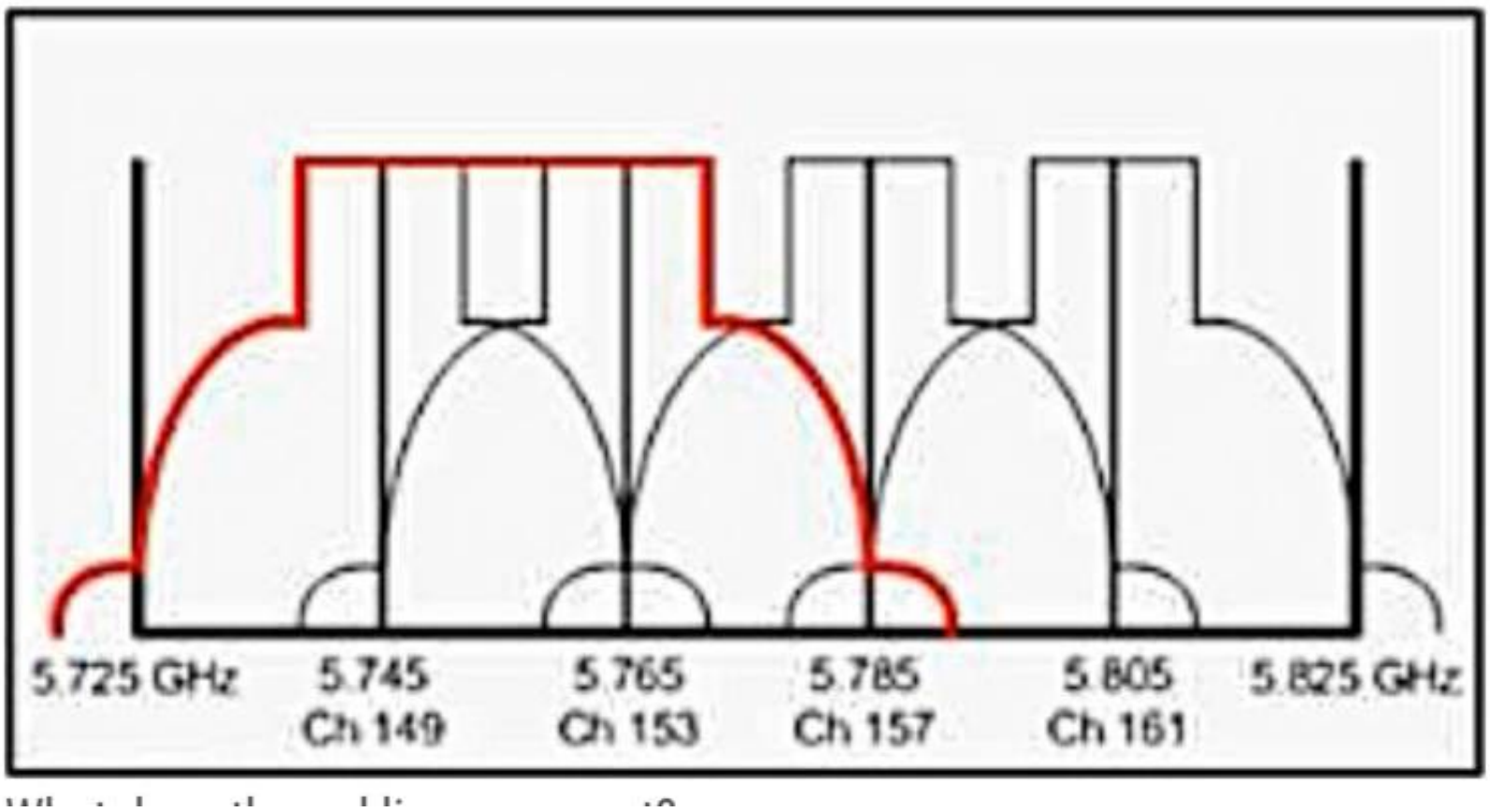
NEW QUESTION 10
Which two management services support connecting FortiAPs to the FortiPresence cloud? (Choose two.

A. FortiSASE
B. FortiGate
C. FortiLAN Cloud
D. FortiSwitch Manager

Answer: BC

Explanation:
FortiPresenceis Fortinet's Wi-Fi analytics/cloud presence platform.
FortiAPs can be managed directly byFortiGateorFortiLAN Cloudand connect their analytics/events to the FortiPresence cloud for presence analytics.
FortiSASEandFortiSwitch Managerdo not provide FortiPresence integration for APs.

NEW QUESTION 12
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 15
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 18
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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