Fortinet

Exam Questions FCP_FWF_AD-7.4

FCP - Secure Wireless LAN 7.4 Administrator

NEW QUESTION 1
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 2
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 3
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)

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

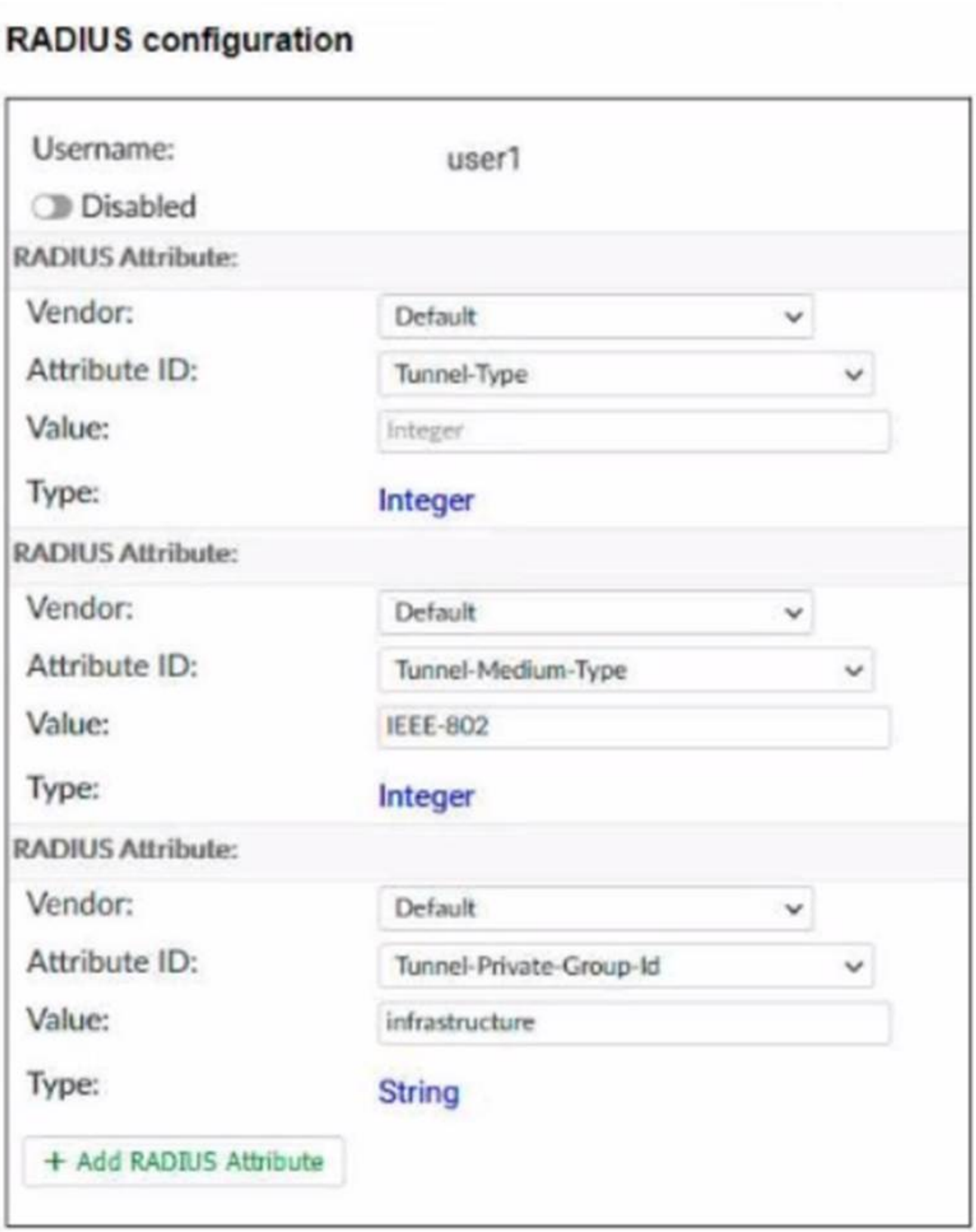
Answer: BC

Explanation:
For advanced wireless troubleshooting:
Capturing air traffic (B): This means performing a wireless packet capture (sniffing), usually via the FortiAP's diagnostic tools (e.g., cw_diag sniff), to see low-level association/authentication issues, interference, or protocol errors.
Reviewing event logs (C): Check event logs on the FortiGate and FortiAP to find authentication failures, disconnections, roaming events, or system messages specific to the wireless station.
A (creating/assigning a new profile) is not typically an advanced troubleshooting step; it's more of a configuration or workaround.
D (collecting power management info) is rarely required except for specific power-saving issues, and is not a primary advanced troubleshooting step.

NEW QUESTION 4
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 5
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 6
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 7
Refer to the exhibit.

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

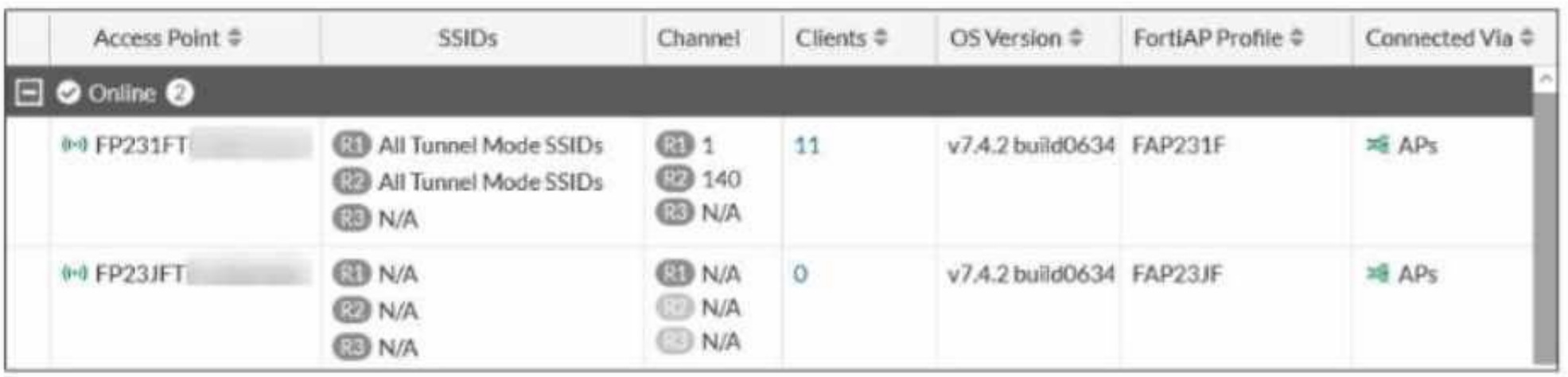
A. The channels will be scanned by the wireless intrusion detection system (WIDS)
B. The channels cannot be used because of regulatory channel restrictions
C. The channels can be used only when Radio Resource Provisioning is enabled
D. The channels are subject to dynamic frequency selection (DPS) regulations

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
Refer to the exhibit.



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?

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

Explanation:
Comprehensive Detailed Step by Step Explanation from all your Knowledge and Guides availableExhibit Analysis:
The screenshot displays two FortiAPs (FP231FT and FP23JFT) in the wireless controller??s managed APs list. Both APs are online and connected via APs.
FP231FT shows active SSIDs (??All Tunnel Mode SSIDs??) and has 11 clients connected. FP23JFT shows ??N/A?? for all SSIDs and ??0?? clients.
Diagnosis:
??N/A?? for SSIDs on FP23JFT clearly indicates it is not broadcasting any SSID.
Both APs are running the same OS version and have their respective FortiAP profiles assigned. Evaluating the Options:
* A. Enable the radios on the FAP23JF FortiAP profile.
Correct: If the radios (2.4GHz/5GHz) are disabled in the FortiAP profile, the AP will not broadcast any SSID, resulting in ??N/A?? and ??0 clients??. This is a common issue seen in FortiOS Wireless LAN management.
This matches the symptom, as the AP is online (communicating with the controller), but has no active radio (hence, no SSID is broadcasted).
* B. Replace the FortiAP device model to match the other device.
Incorrect. FortiOS supports different models in the same deployment, as long as the correct profile is applied.
* C. Disable the override setting on the FortiAP that is preventing it from broadcasting SSIDs.
Misleading. Unless an override has specifically disabled SSID broadcasting, this is not directly indicated by the screenshot. Usually, radio disabled at profile is the root cause.
* D. Assign the FAP231F FortiAP profile to the problematic FortiAP device.
Incorrect. The correct profile (FAP23JF) is already assigned to FP23JFT; assigning a mismatched profile can cause more issues and is not best practice.
Guide Reference & Reasoning:
FortiOS Administration Guide – Wireless Section:
When an AP is online but SSIDs are not broadcasted and ??N/A?? appears for radio slots, it strongly points to the radios being disabled in the FortiAP profile (see Wireless Controller > Managed FortiAPs).
The guide explains that ??If the radios are disabled in the profile, the AP will not broadcast any SSID. To resolve, enable the radios (2.4GHz, 5GHz) in the FortiAP profile and reapply or reboot the AP??.
FortiAP Profile Settings:
Go to WiFi & Switch Controller > FortiAP Profiles. Edit the FAP23JF profile.
Check both ??Radio 1?? and ??Radio 2?? (enable if disabled). Save the changes and ensure the profile is pushed to the AP. Typical Steps to Fix:
Log into the FortiGate.
Navigate to WiFi & Switch Controller > FortiAP Profiles. Edit the FAP23JF profile.
Under the radio settings, ensure both radios are set to ??Enable??.
Apply the changes.
The AP will now broadcast the SSIDs as configured. Summary:
The problem is caused by disabled radios in the FAP23JF FortiAP profile. Enabling the radios in the profile will allow the AP to start broadcasting SSIDs.
Final Answer A. Enable the radios on the FAP23JF FortiAP profile.

NEW QUESTION 9
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.

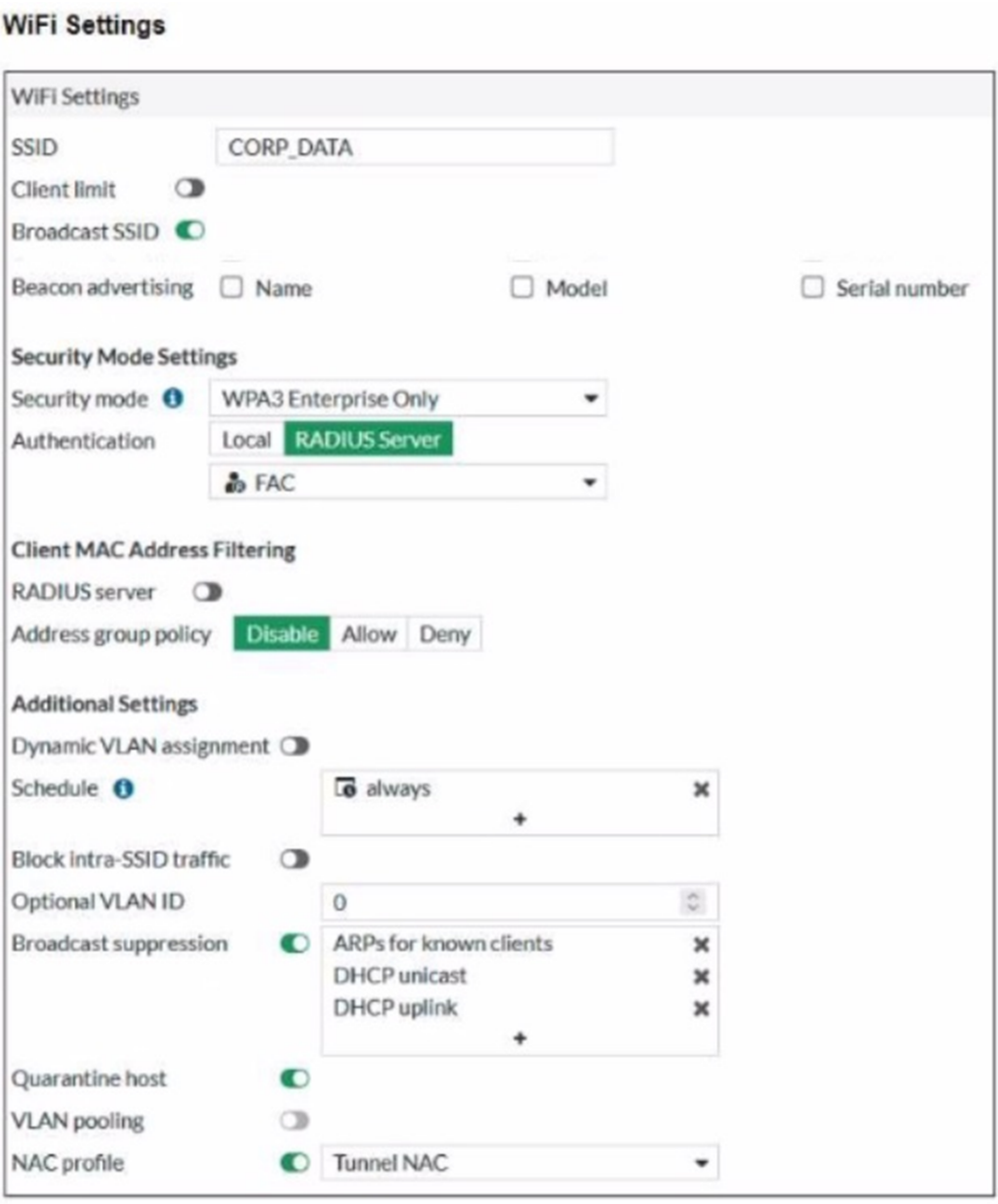
NEW QUESTION 10
Which security solution can you implement in the Security Fabric to identify and prevent threats?

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.

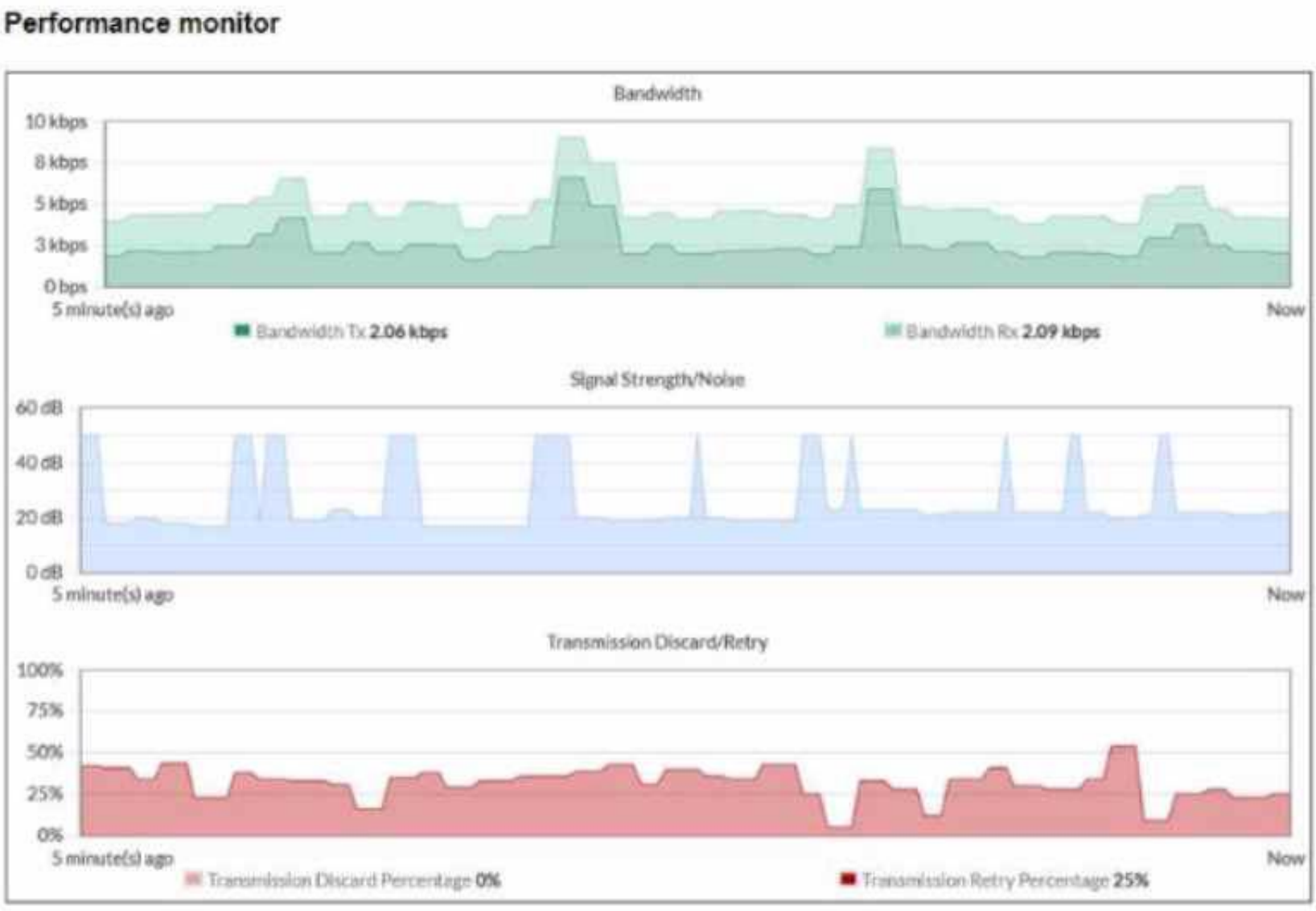
Answer: A

NEW QUESTION 11
How can you find the upstream and downstream link rates of a wireless client connected to a FortiAP?

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

NEW QUESTION 13
Exhibit.



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

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

NEW QUESTION 16
Which two rotes does FortiPresence analytics assist in generating presence reports" (Choose two.)

A. Gathering details about on-site guest users
B. Reporting potential threats by on-site guest users
C. Comparing current data with historical records
D. Predicting the number of on-site guest users

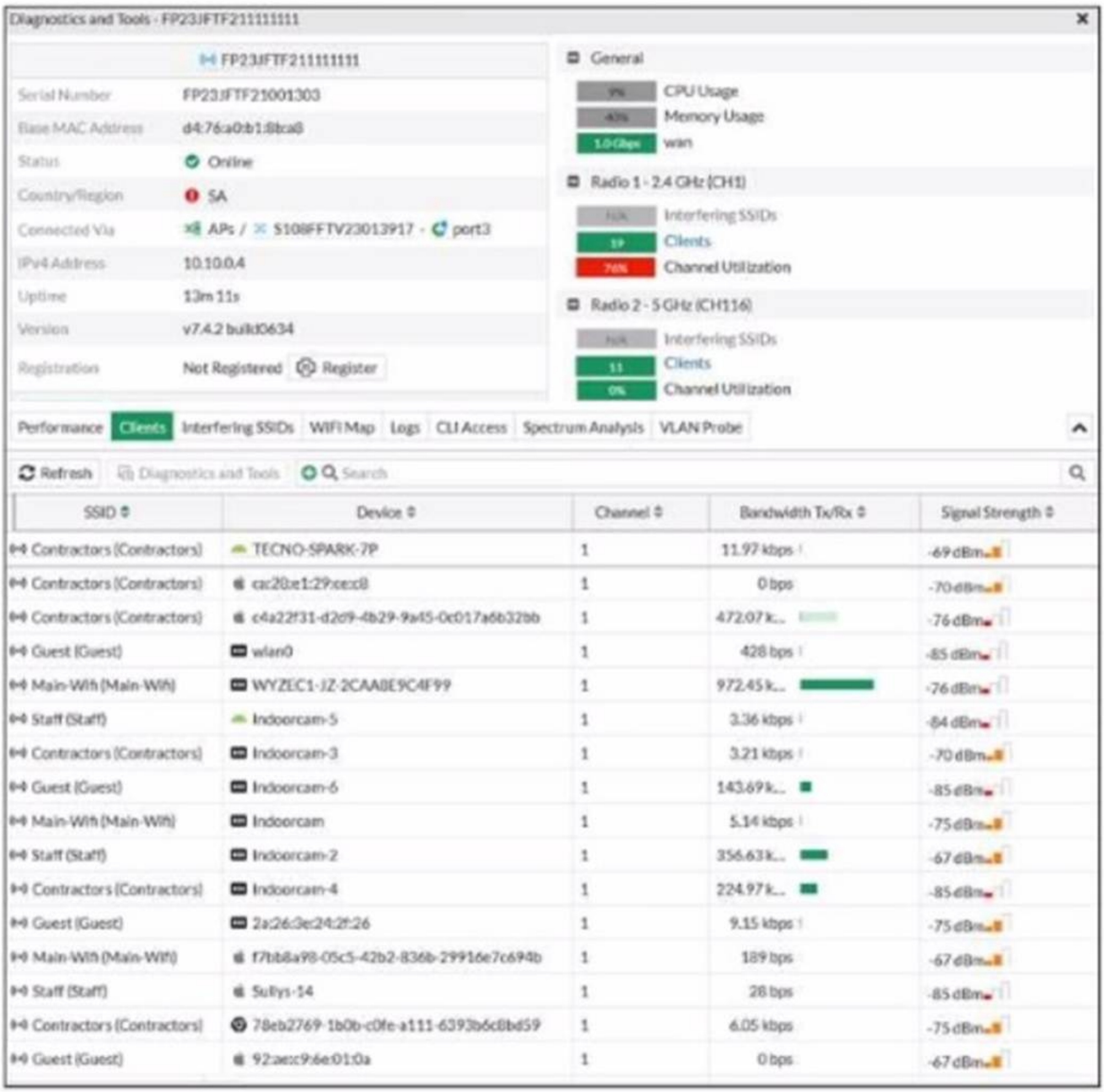
Answer: AC

Explanation:
FortiPresence analytics is a platform for presence analytics—monitoring WiFi user presence, dwell time, and visitor trends in physical spaces.
A: It collects and reports details about on-site guest users, such as visit duration and repeat visits.
C: It enables comparison of current user presence and activity data with historical trends, supporting operational and marketing analysis.
B (reporting potential threats) is not a function of presence analytics.
D (predicting future guest counts) is not a core function; FortiPresence reports on actual and historical data, not predictive analytics.

NEW QUESTION 17
Refer to the exhibits.

```
61E-01 # get wireless-controller rf-analysis
WTP: FP23JFTF21111111  0-10.10.0.2:15246
     channel    rssi-total   rf-score     overlap-ap   interfere-ap chan-utilizaion
           1       275           1            8            7              91%
           2       73            8            0            9              80%
           3       49            10           0            11             62%
           4       80            7            5            11             54%
           5       45            10           1            11             69%
           6       77            8            2            8              49%
           7       55            9            2            14             65%
           8       24            10           0            14             57%
           9       29            10           0            12             58%
          10       59            9            1            11             61%
          11       180           1            9            9              48%
          12       43            10           0            7              38%
          13       19            10           0            7              58%
          14       8             10           0            7              49%
          36       26            10           2            2              39%
         100       249           1            3            3              89%
         116       72            8            2            2              68%
         149       44            10           3            3              54%
```

Diagnostic summary of the AP and neighboring APs



The exhibits show the AP profile the controller RF analysis output and a diagnostic summary of the AP and neighboring APs
The wireless network is used for multiple purposes including corporate access guest access and connecting point-of-sale and loT devices Users connecting to the guest network located in the reception area are reporting stow performance
Which configuration change is most likely to improve performance?

A. Reduce the number of SSIDs being broadcast by the reception AP
B. Enable frequency handoff on the AP to band steer clients
C. increase the transmission power of the AP radios
D. install another AP in the reception area to improve available bandwidth.

Answer: A

Explanation:
Analysis of Exhibits:
RF Analysis:
Channel 1 (2.4 GHz) shows very high utilization (91%) and significant overlap/interference from other APs (8 overlap-AP, 7 interfere-AP).
Channel utilization on 2.4 GHz is very high, indicating congestion and contention.
AP Diagnostic Summary:
Radio 1 (2.4 GHz):
Channel Utilization: 78%
Interfering SSIDs: 18

A long list of clients and many SSIDs being broadcast on Channel 1.
Radio 2 (5 GHz):
Channel Utilization: 0% (much lower usage; likely not all clients or SSIDs are using it).
SSID List:
Multiple SSIDs are being broadcast by the AP, which increases management overhead (beacon /probe traffic) and reduces airtime for actual data.
Problem Symptoms:
Guest users in the reception area (on 2.4 GHz, channel 1) are experiencing slow performance.
Option Analysis:
* A. Reduce the number of SSIDs being broadcast by the reception AP
Correct.
Each SSID adds additional management overhead (beacons, probes) that consume airtime on already congested 2.4 GHz channels.
Reducing the number of SSIDs frees up airtime for actual client data, which can improve throughput and reduce latency, especially in high-density environments with high channel utilization.
This is a recommended best practice for optimizing Wi-Fi performance in congested environments.
* B. Enable frequency handoff on the AP to band steer clients
Helpful if clients support 5 GHz, but not all client devices (especially IoT/guests) do; with such high channel utilization, this is a secondary optimization.
* C. Increase the transmission power of the AP radios
This can make interference worse and does not solve airtime congestion; it may also increase contention with neighboring APs.
* D. Install another AP in the reception area to improve available bandwidth
Adding more APs on congested channels can actually increase interference and may not help unless channel planning and SSID management are also addressed.
Summary:
Reducing the number of SSIDs is the most direct, configuration-based action that will improve available airtime and performance for clients in a congested, high-utilization environment like the one shown in the exhibits.

NEW QUESTION 22
.....

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

100% Actual & Verified — Instant Download, Please Click
Order The FCP_FWF_AD-7.4 Practice Test Here