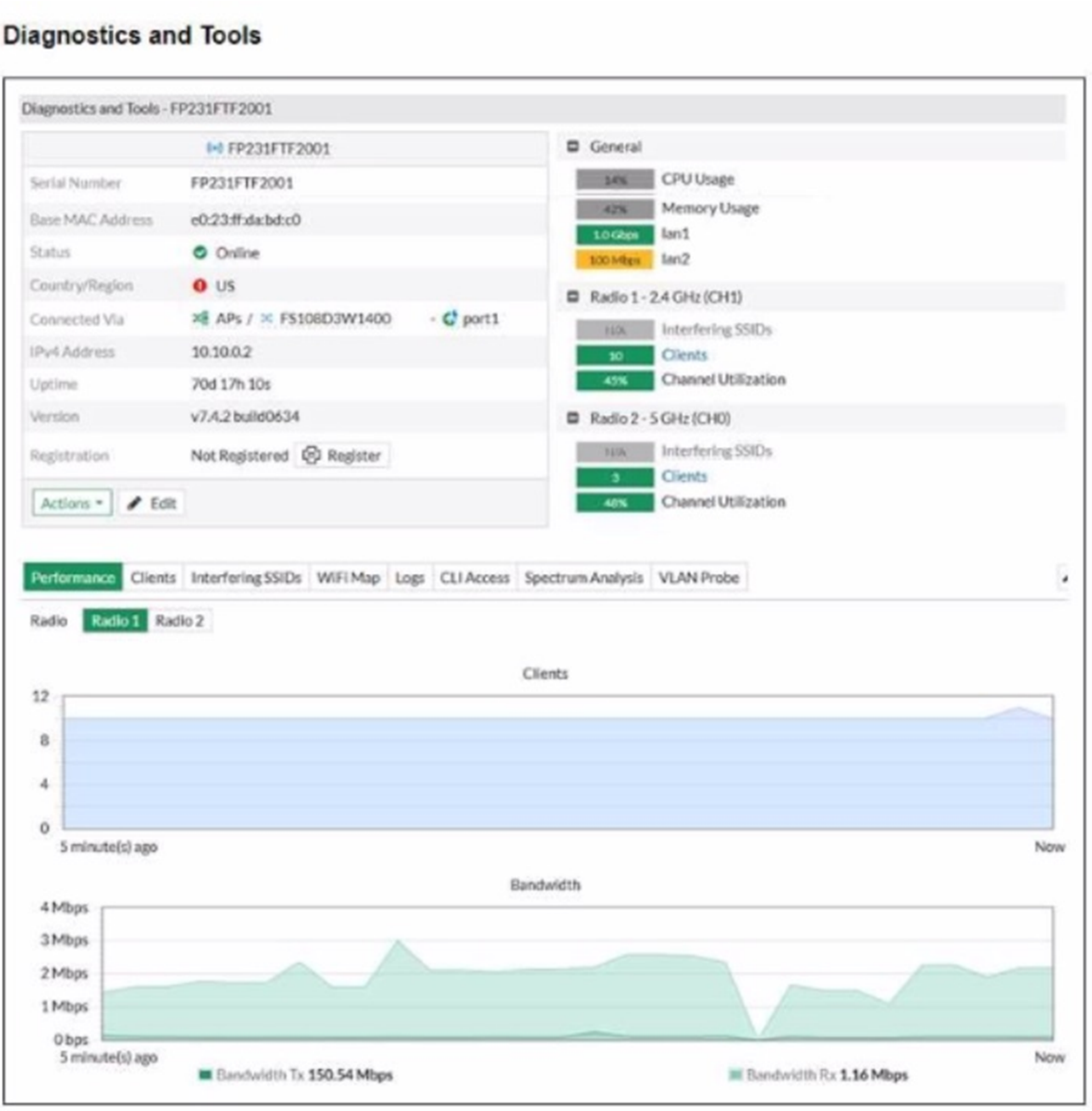
Fortinet

Exam Questions FCP_FWF_AD-7.4

FCP - Secure Wireless LAN 7.4 Administrator

NEW QUESTION 1
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?

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

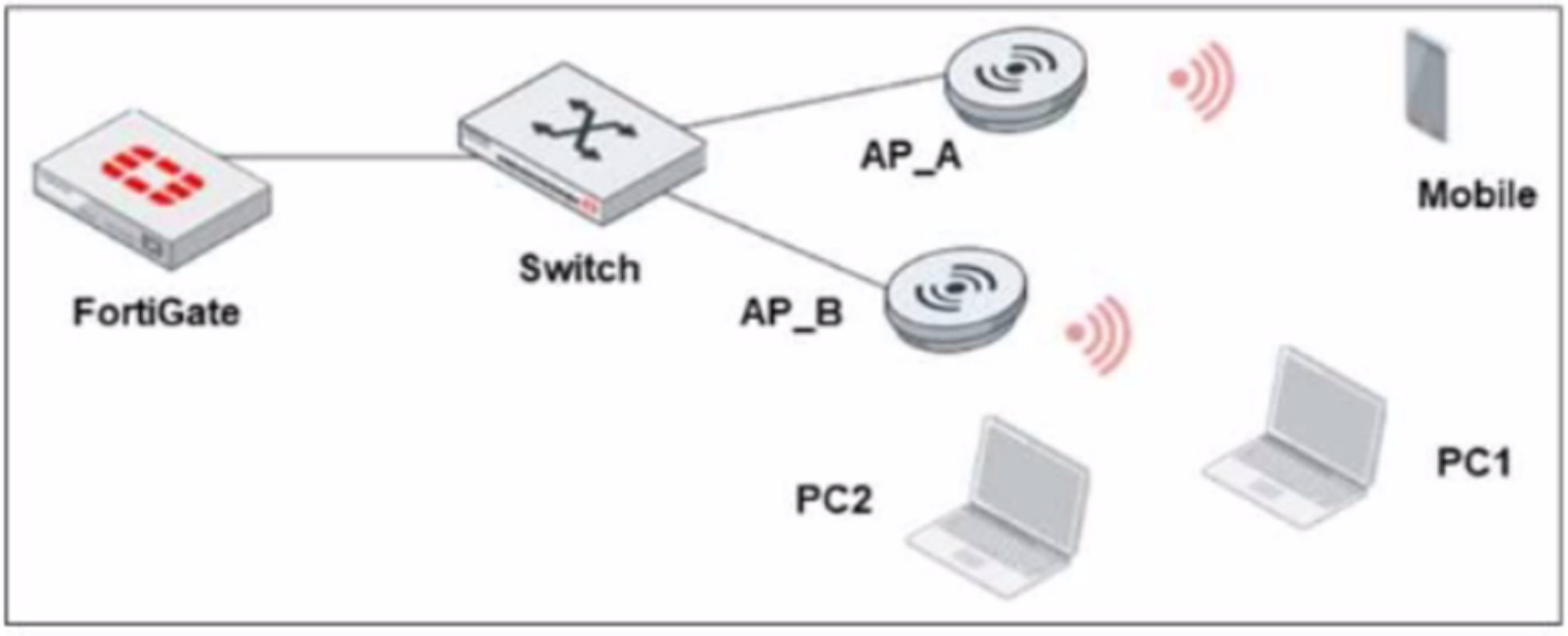
Answer: A

Explanation:

Exhibit Review:
The diagnostics panel for FortiAP FP231FTF2001 shows:
Tx bandwidth label: 150.54 Mbps (likely the negotiated or theoretical maximum).
Bandwidth graph (actual traffic): Transmit (Tx) bandwidth peaked at only ~3 Mbps over the last 5 minutes—far below the maximum.

Radio 1 (2.4 GHz) shows 10 interfering SSIDs and 40% channel utilization.
Radio 2 (5 GHz) is not the focus in the current graph.
Interpretation:
The significant difference between the potential (label) and actual (graph) throughput indicates that something is preventing the AP from delivering full speed.
This could be resource overload (e.g., too many clients, too much interference, CPU/memory constraints), leading to overall reduced throughput for all users.
The graph represents real-time/actual usage, not just the theoretical capability. Option Breakdown:
* A. Resources on FortiAP are overloaded which limits speed rates for all users
Correct. Overload (either due to too many clients, high interference, or hardware resources) is a logical reason why actual throughput is far below the possible maximum.
* B. Label values are historical and provide average bandwidth
Incorrect. The label reflects the maximum link rate or negotiated data rate, not an average or historical usage value.
* C. FortiAP is dual band and is transmitting data faster with a higher frequency band
Not supported by the evidence. The current data is for Radio 1 (2.4 GHz) and does not show high usage on either band.
* D. Bandwidth is shared with other SSID signals broadcasting for nearby AP devices
While interference does share airtime, the drastic drop in throughput strongly suggests an overload or other limiting factor on this AP.
Summary:
The large gap between the expected maximum (label) and the actual throughput observed suggests that resource overload is the root cause of poor wireless speeds for all users.

NEW QUESTION 2
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 3
Refer to the exhibit.

Wireless controller debug output

```
61E-01 # 55385.062 192 9a:c5:d1:5f:54:70 <ih> IEEE 802
55385.063 192 9a:c5:d1:5f:54:70 <ih> 9a:c5:d1:5f:54:70 ver=1 type=0 (EAP_PACKET) data len=10
55385.063 192 9a:c5:d1:5f:54:70 <ih> IEEE 802.11 mgmt: 0) ==> RADIUS Server code=1 (Access-Request) id=40 len=291
55385.063 192 9a:c5:d1:5f:54:70 <ih> IEEE 802.11 mgmt: 0) <== RADIUS Server code=11 (Access-Challenge) id=40 len=79
55385.064 192 9a:c5:d1:5f:54:70 <dc> STA add 9a:c5:d1: ver=2 type=0 (EAP_PACKET) data len=33
55385.064 192 9a:c5:d1:5f:54:70 <cc> STA_CFG_REQ(68) s B) ==> 9a:c5:d1:5f:54:70 ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3
98015.066 9a:c5:d1:5f:54:70 <eh>     ***9a:c5:d1:5f:54 B) <== 9a:c5:d1:5f:54:70 ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3
98015.066 9a:c5:d1:5f:54:70 <eh>     send IEEE 802.1X ver=1 type=0 (EAP_PACKET) data len=8
98015.066 9a:c5:d1:5f:54:70 <eh> IEEE 802.1X (EAPOL 14 0) ==> RADIUS Server code=1 (Access-Request) id=41 len=295
55385.066 192 9a:c5:d1:5f:54:70 <cc> STA add 9a:c5:d1: 0) <== RADIUS Server code=11 (Access-Challenge) id=41 len=52
55385.067 192 9a:c5:d1:5f:54:70 cwAcStaRbtAdd: I2C_STA ver=2 type=0 (EAP_PACKET) data len=6
55385.069 192 9a:c5:d1:5f:54:70 <cc> STA_CFG_RESP(68) B) ==> 9a:c5:d1:5f:54:70 ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3
98015.189 9a:c5:d1:5f:54:70 <eh> IEEE 802.1X (EAPOL 14 5B) <== 9a:c5:d1:5f:54:70 ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3
98015.189 9a:c5:d1:5f:54:70 <eh>     recv IEEE 802.1X ver=1 type=0 (EAP_PACKET) data len=161
98015.190 9a:c5:d1:5f:54:70 <eh> RADIUS message (type= 0) ==> RADIUS Server code=1 (Access-Request) id=42 len=448
98015.192 9a:c5:d1:5f:54:70 <eh> RADIUS message (type= 0) <== RADIUS Server code=11 (Access-Challenge) id=42 len=1459
98015.192 9a:c5:d1:5f:54:70 <eh>     send IEEE 802.1X ver=2 type=0 (EAP_PACKET) data len=1403
98015.193 9a:c5:d1:5f:54:70 <eh> IEEE 802.1X (EAPOL 37 B) ==> 9a:c5:d1:5f:54:70 ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3
98015.210 9a:c5:d1:5f:54:70 <eh> IEEE 802.1X (EAPOL 12 5B) <== 9a:c5:d1:5f:54:70 ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3
98015.210 9a:c5:d1:5f:54:70 <eh>     recv IEEE 802.1X ver=1 type=0 (EAP_PACKET) data len=111
98015.211 9a:c5:d1:5f:54:70 <eh> RADIUS message (type= 0) ==> RADIUS Server code=1 (Access-Request) id=48 len=398
98015.212 9a:c5:d1:5f:54:70 <eh> RADIUS message (type= 0) <== RADIUS Server code=11 (Access-Challenge) id=48 len=157
98015.212 9a:c5:d1:5f:54:70 <eh>     send IEEE 802.1X ver=2 type=0 (EAP_PACKET) data len=111
98015.213 9a:c5:d1:5f:54:70 <eh> IEEE 802.1X (EAPOL 10 5B) ==> 9a:c5:d1:5f:54:70 ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3
98015.244 9a:c5:d1:5f:54:70 <eh> IEEE 802.1X (EAPOL 16 B) <== 9a:c5:d1:5f:54:70 ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3
98015.245 9a:c5:d1:5f:54:70 <eh>     recv IEEE 802.1X ver=1 type=0 (EAP_PACKET) data len=59
98015.246 9a:c5:d1:5f:54:70 <eh> RADIUS message (type= 0) ==> RADIUS Server code=1 (Access-Request) id=49 len=346
98015.602 9a:c5:d1:5f:54:70 <eh> RADIUS message (type= 0) <== RADIUS Server code=3 (Access-Reject) id=49 len=44
98015.603 9a:c5:d1:5f:54:70 <eh>     send IEEE 802.1X ver=2 type=0 (EAP_PACKET) data len=4
98022.931 9a:c5:d1:5f:54:70 <eh> IEEE 802.1X (EAPOL 83 ) ==> 9a:c5:d1:5f:54:70 ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3
98022.936 9a:c5:d1:5f:54:70 <eh> IEEE 802.1X (EAPOL 11 d1:5f:54:70 DISCONNECTED***
98022.936 9a:c5:d1:5f:54:70 <eh>     recv IEEE 802.1X ( (0-10.10.0.2:15246)  9a:c5:d1:5f:54:70 ret -1
98022.938 9a:c5:d1:5f:54:70 <eh> RADIUS message (type= 5f:54:70 ws (0-10.10.0.2:15246) vap WLAN_NET rId 1 wId 3
98022.940 9a:c5:d1:5f:54:70 <eh> RADIUS message (type= :deauth ==> 9a:c5:d1:5f:54:70 ws (0-10.10.0.2:15246) vap WLAN_NET rId 1 wId 3 e0:23:ff:da:bd:d3
98022.941 9a:c5:d1:5f:54:70 <eh>     send IEEE 802.1X ta 9a:c5:d1:5f:54:70 del ==> ws (0-10.10.0.2:15246) rId 1 wId 3
98022.941 9a:c5:d1:5f:54:70 <eh> IEEE 802.1X (EAPOL 11 5f:54:70 vap WLAN_NET ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3 sec WPA3 ENTERPRISE TRANSITION reason E2C_STA_DISAUTH
98022.946 9a:c5:d1:5f:54:70 <eh> IEEE 802.1X (EAPOL 63 _DEL remove sta 9a:c5:d1:5f:54:70 10.10.0.2/1/3/1 from staRbt
98022.947 9a:c5:d1:5f:54:70 <eh>     recv IEEE 802.1X 5f:54:70 vap WLAN_NET ws (0-10.10.0.2:15246) rId 1 wId 3 bssid e0:23:ff:da:bd:d3 NON-AUTH
98022.948 9a:c5:d1:5f:54:70 <eh> RADIUS message (type= :c5:d1:5f:54:70 vap WLAN_NET ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3 sec WPA3 ENTERPRISE TRANSITION user user1 group NULL
98022.949 9a:c5:d1:5f:54:70 <eh> RADIUS message (type= 5f:54:70 vap WLAN_NET ws (0-10.10.0.2:15246) rId 1 wId 3 bssid e0:23:ff:da:bd:d3 NON-AUTH
                                                    :c5:d1:5f:54:70 vap WLAN_NET ws (0-10.10.0.2:15246) rId 1 wId 3 e0:23:ff:da:bd:d3 sec WPA3 ENTERPRISE TRANSITION user user1 group NULL
                                                    9a:c5:d1:5f:54:70 <== ws (0-10.10.0.2:15246) rc 0 (Success)
```

The wireless client connects to the wireless network on WLAN_NET tunnel mode interface The exhibit stows the client exchange communication with the wireless controller and the RADIUS server
Which two issues can you observe in the wireless station debug outputs (Choose two.)

A. The wireless client has an unsuccessful association with the wireless controller
B. The wireless client has failed to complete the four-way handshake process.
C. The wireless client has denied the connection after many failed trials
D. The wireless client has incorrect credentials to authenticate with the authentication server

Answer: BD

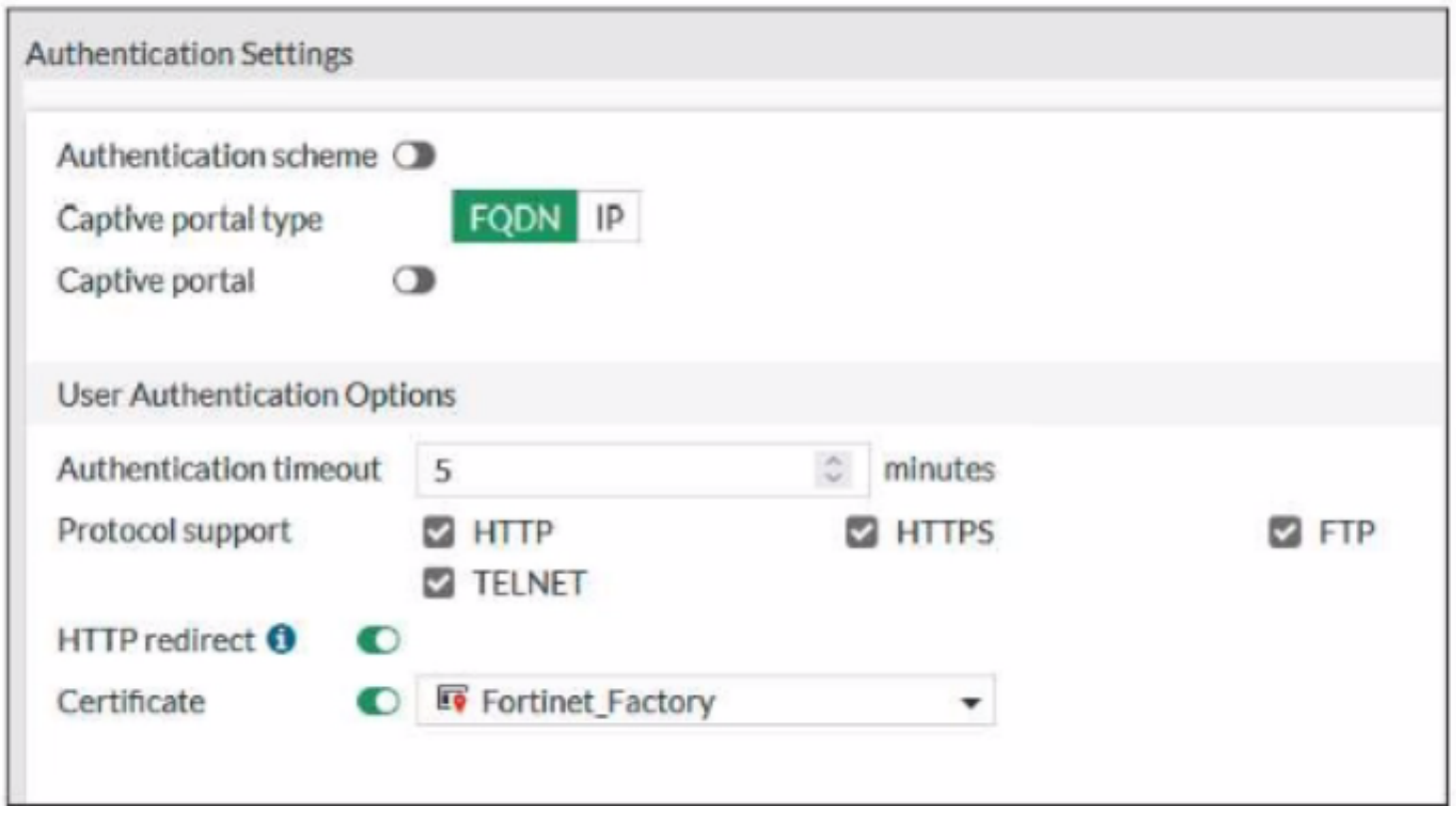
Explanation:
Debug Output Review:
The logs show repeated attempts to connect, with multiple msg: WPA ENTERPRISE TRANSITION and WPA NON-ENTERPRISE TRANSITION events.
There are repeated authentication frame exchanges, but several entries show failure messages, including incomplete handshake and RADIUS/authentication failures.
The client is unable to complete the full authentication process—typical indicators of incorrect credentials (failed RADIUS authentication) and failure in the WPA handshake process.
Unsuccessful association—No; the client does associate but fails at authentication/handshake.
* C. Client denied after many attempts—No evidence the client itself is denying; it??s failing at the network??s authentication step.

NEW QUESTION 4
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 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.

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 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 management services support connecting FortiAPs to the FortiPresence cloud? (Choose two.

A. FortiSASE

B. FortiGate
C. FortiLAN Cloud
D. FortiSwitch Manager

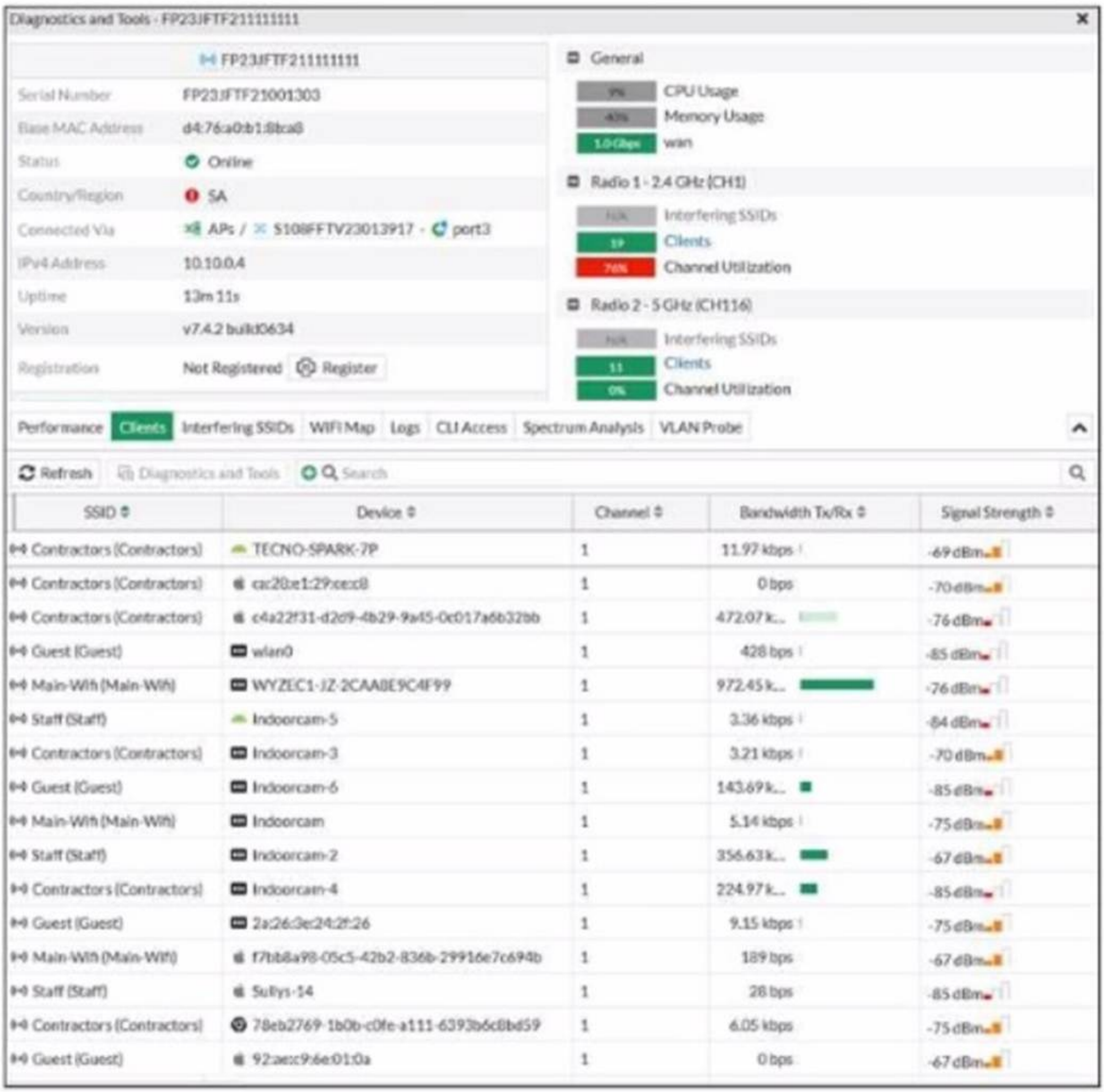
Answer: BC

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 9
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 10
.....

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