Fortinet

Exam Questions FCP_FWF_AD-7.4

FCP - Secure Wireless LAN 7.4 Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

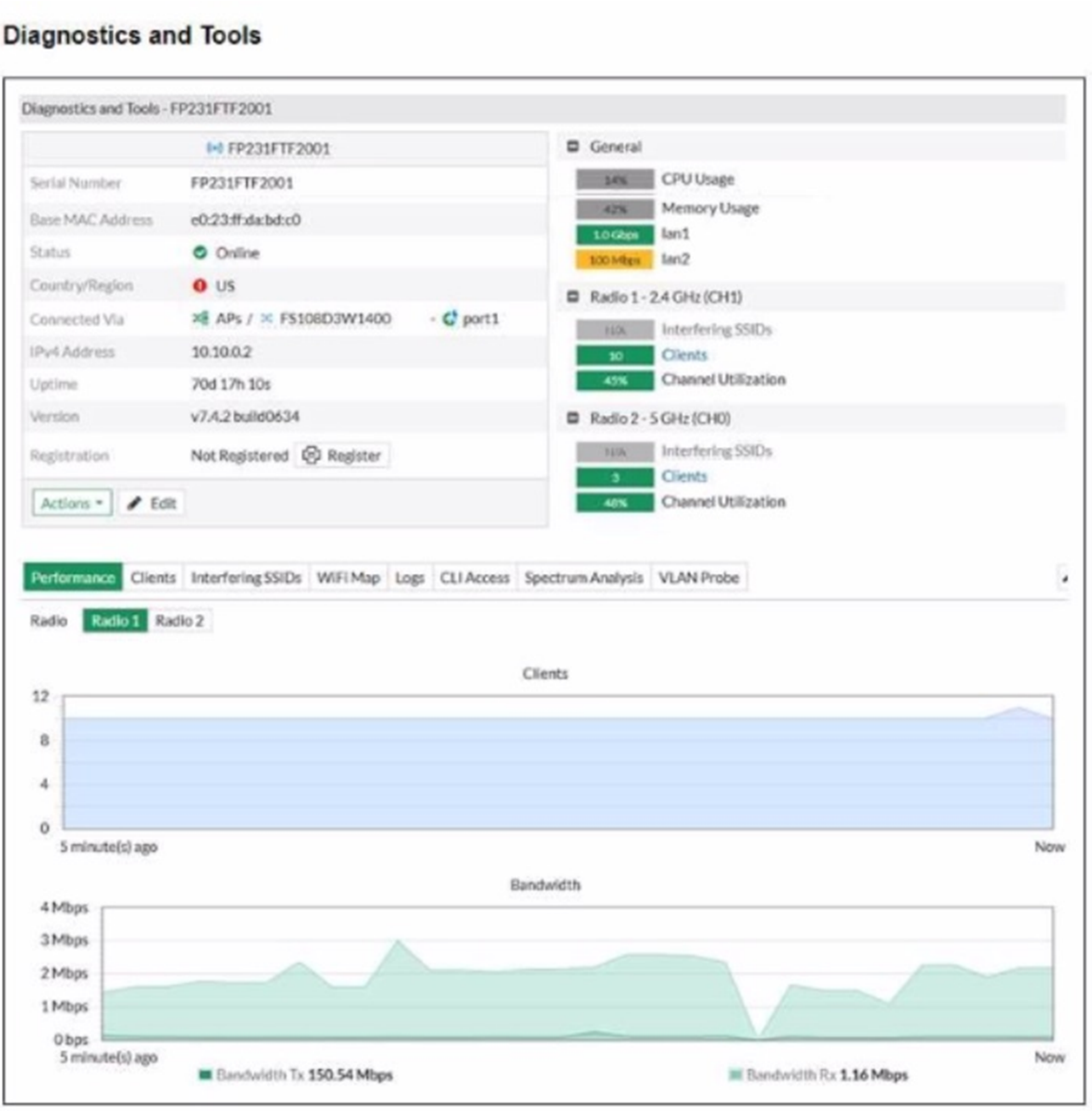
* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

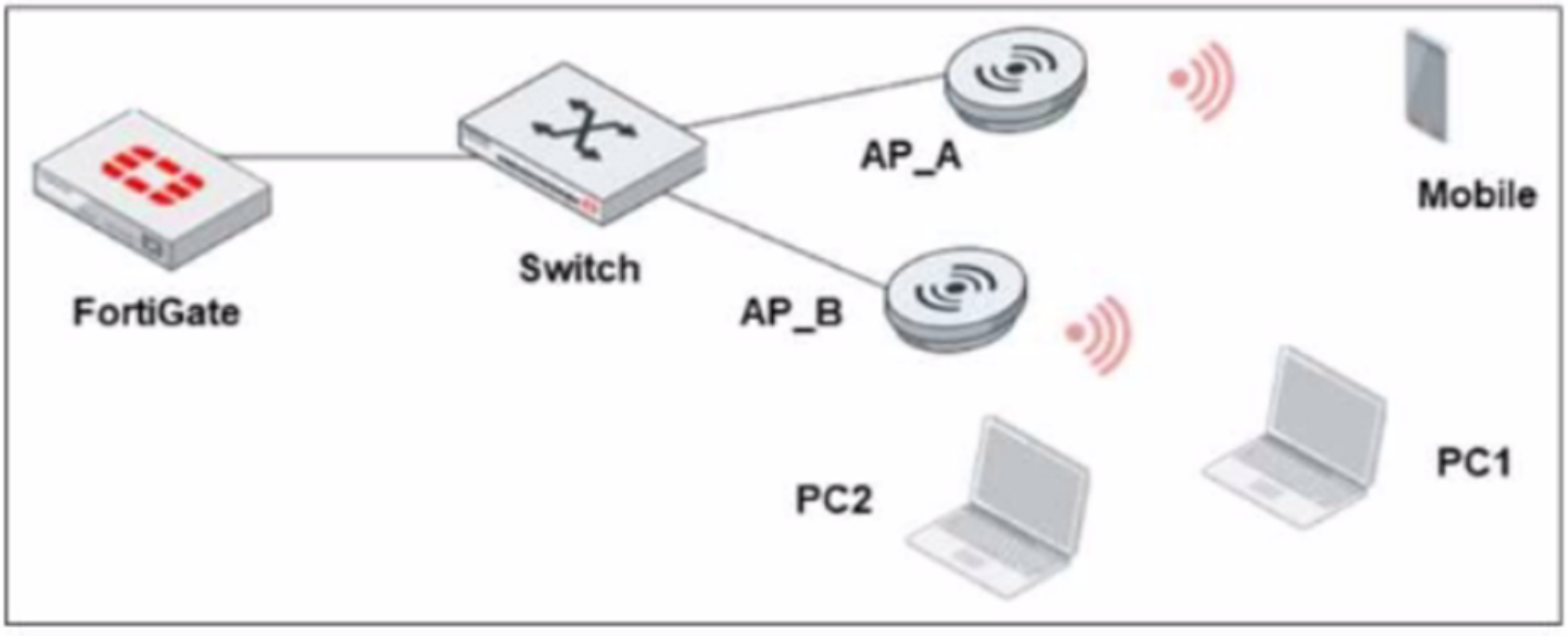
Answer: A

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
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 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
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

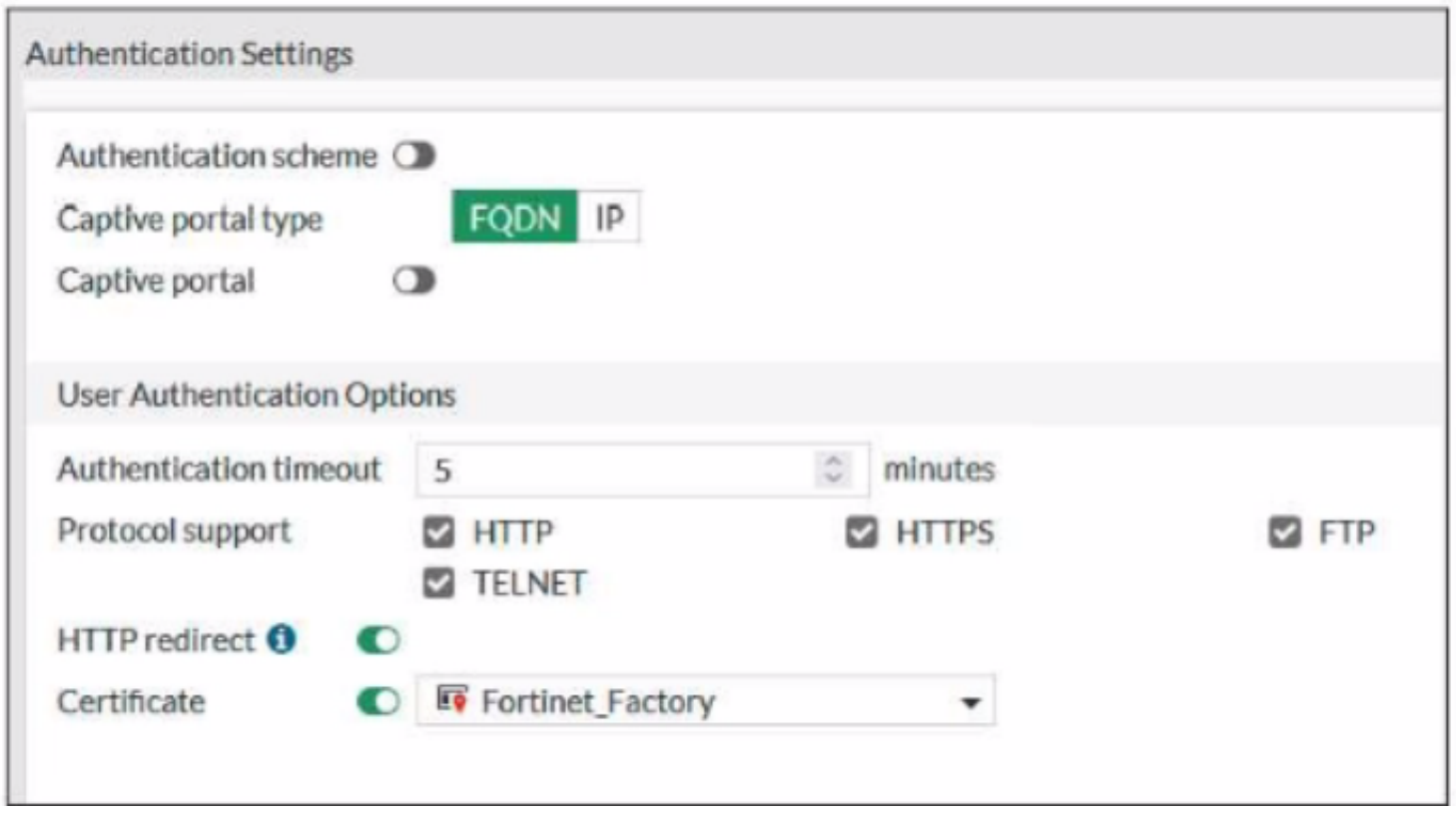
Explanation:
For advanced wireless troubleshooting:
Capturing air traffic (B): This means performing a wireless packet capture (sniffing), usually via the FortiAP's diagnostic tools (e.g., cw_diag sniff), to see low-level association/authentication issues, interference, or protocol errors.
Reviewing 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 6
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 7
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 8
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 9
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 10
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.

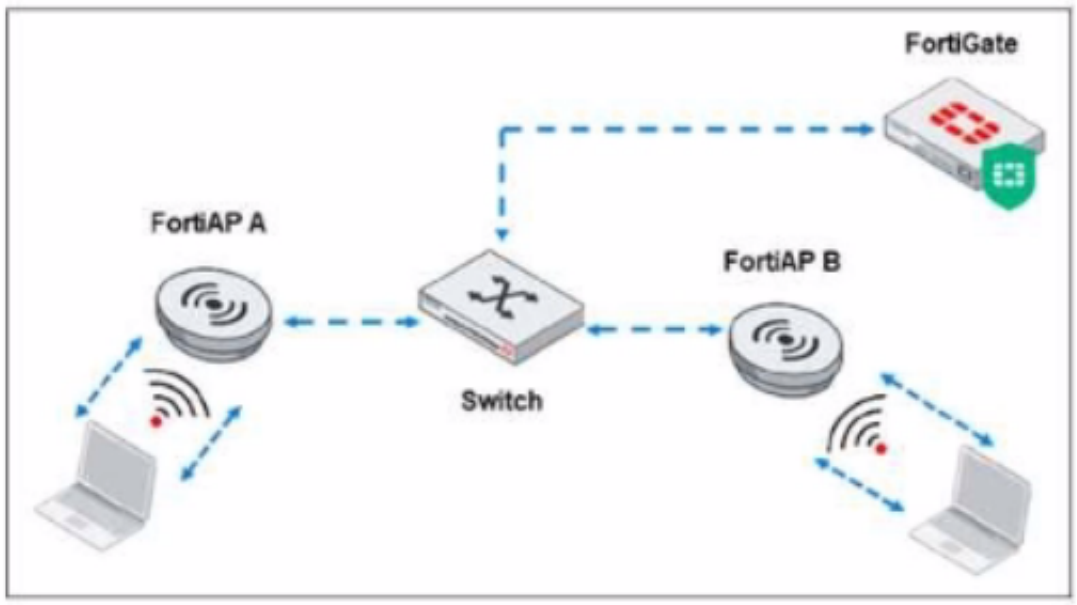
NEW QUESTION 10
Which security solution can you implement in the Security Fabric to identify and prevent threats?

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 14
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 17
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?

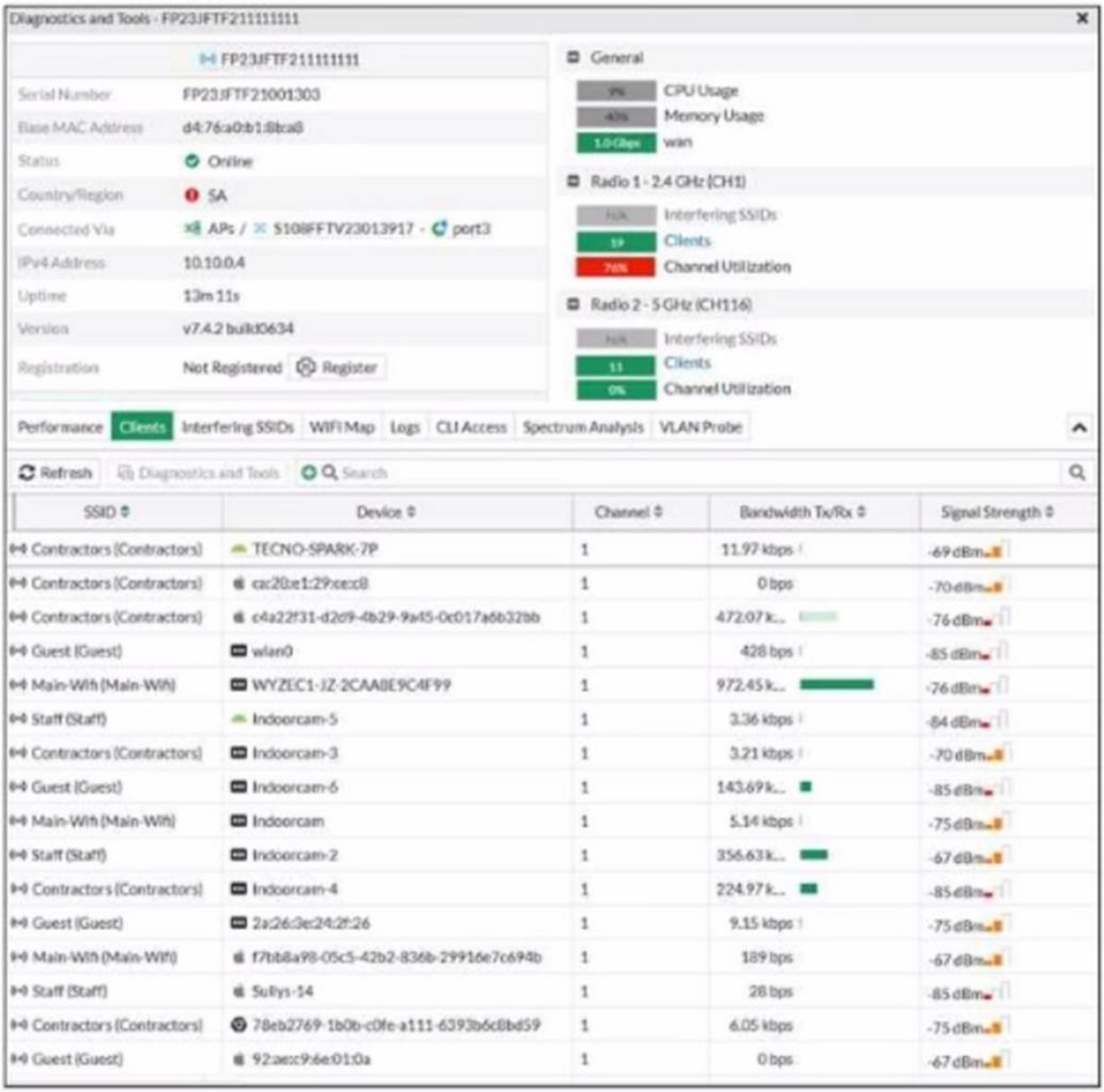
A. The wireless client disconnects and connects to a different, available AP
B. The associated AP marks the wireless client as disconnected and must not reconnect
C. The associated AP sends an alert message to the wireless client about the signal drop
D. The wireless client increases its signal power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

Answer: A

NEW QUESTION 19
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 23
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 24
.....

Relate Links

100% Pass Your FCP_FWF_AD-7.4 Exam with Exambible Prep Materials

https://www.exambible.com/FCP_FWF_AD-7.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/