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.

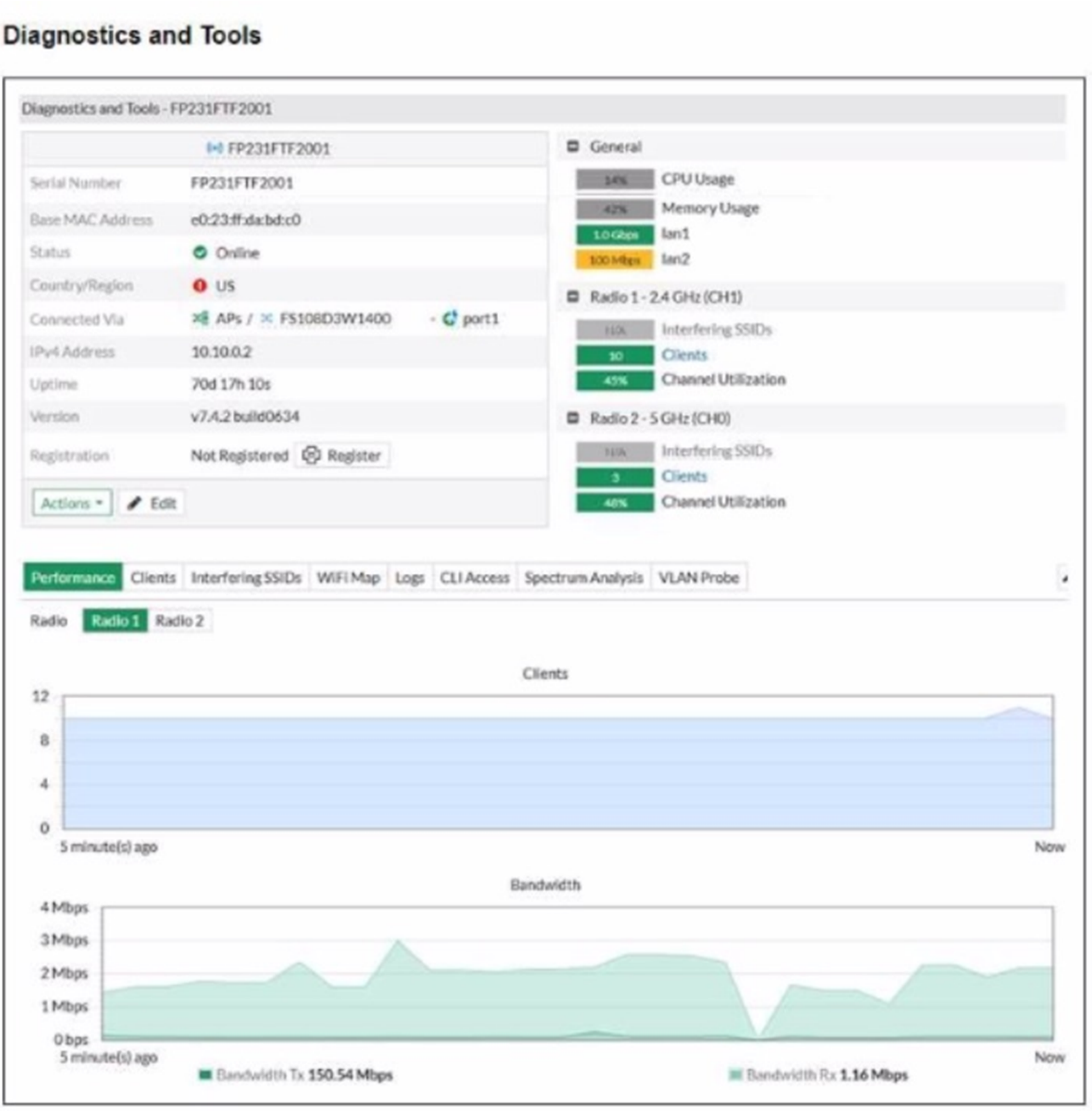
* 100% Pass Rate

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
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

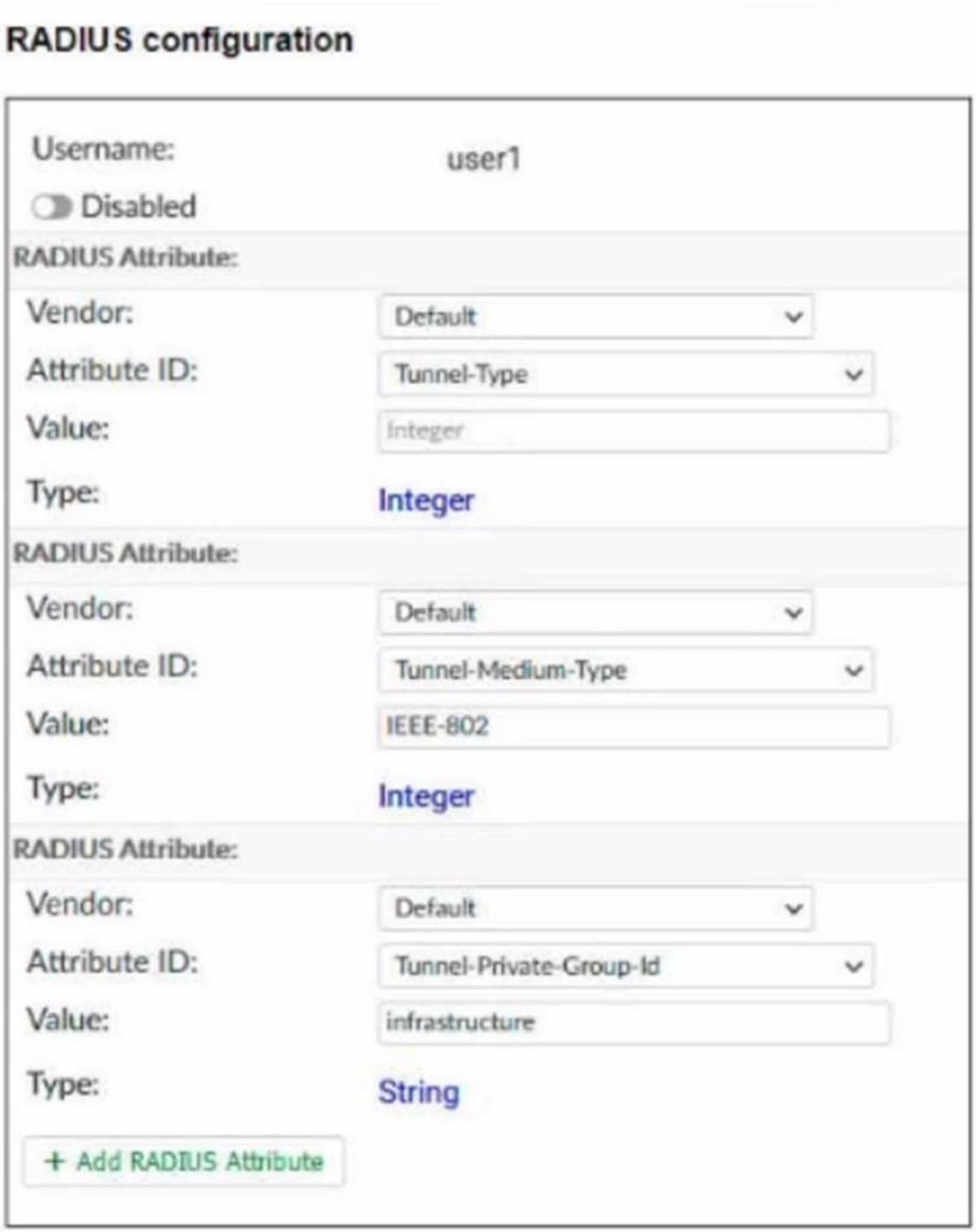
Answer: BC

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 3
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.

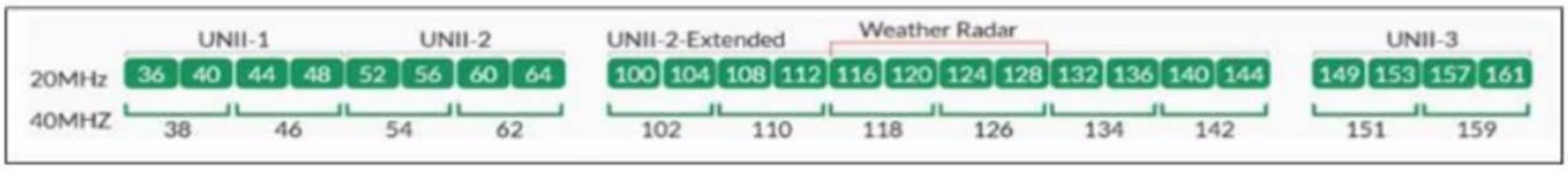
NEW QUESTION 4
An IT department must provide wireless security to employees connected over remote hortiAP devices who must access corporate resources at the mam office
Which action must the IT department take to enforce security policies for all wireless stations accessing corporate resources across 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
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 6
Which security solution can you implement in the Security Fabric to identify and prevent threats?

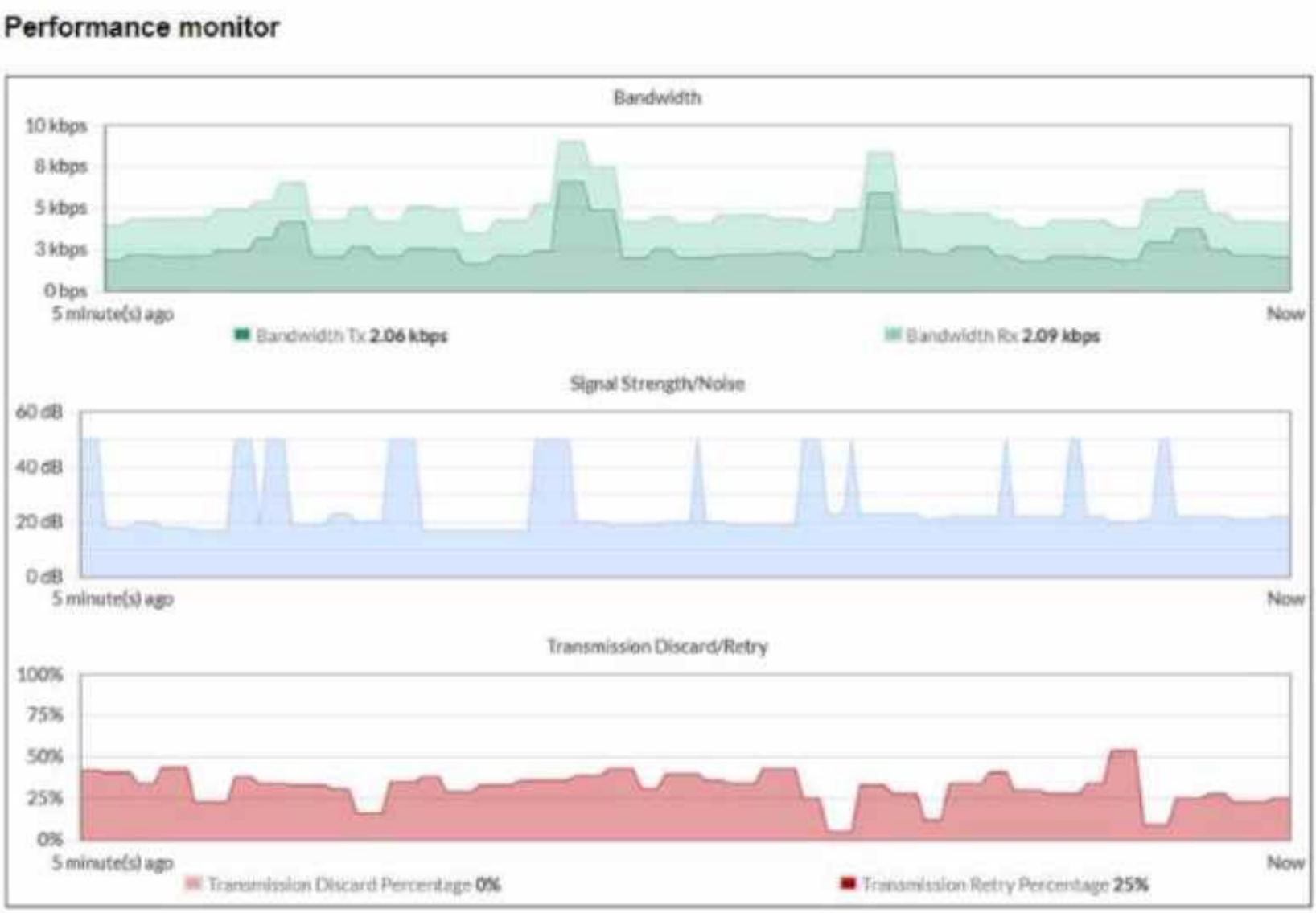
A. Integrated wireless network access
B. Endpoint detection and response
C. Compromised wireless client quarantine
D. Indicator of attack system

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 7
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 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 10
.....

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/