Fortinet.NSE5_FWF_AD-7.6.v2026-09-20.q13

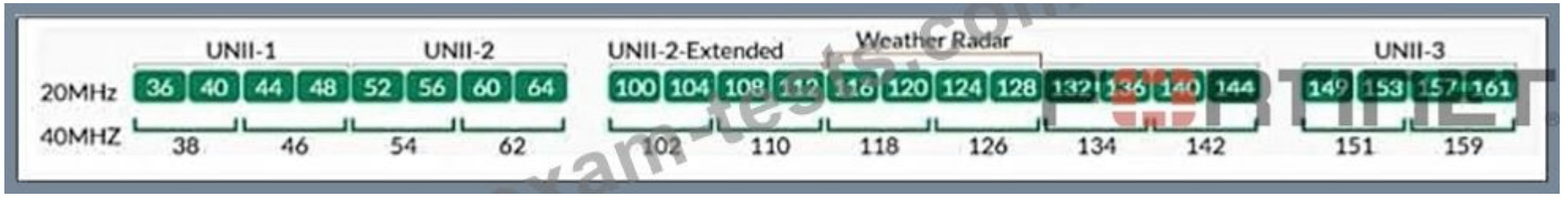
Exam Code:	NSE5_FWF_AD-7.6
Exam Name:	Fortinet NSE 5 - Secure Wireless LAN 7.6 Administrator
Certification Provider:	Fortinet
Free Question Number:	13
Version:	v2026-09-20
# of views:	118
# of Questions views:	130
https://www.exam-tests.com/NSE5_FWF_AD-7.6-exam/Fortinet.NSE5_FWF_AD-7.6.v2026-09-20.q13.html	

NEW QUESTION: 1
Which modulation scheme offers extremely high throughput (EHT) in 802.11be technology?
A. Direct sequence spread spectrum
B. Binary phase-shift keying
C. Orthogonal frequency division multiplexing
D. Quadrature amplitude modulation
Answer: D (LEAVE A REPLY)

NEW QUESTION: 2
Which two statements about a VAP configured for 802.1x Local Authentication are true? (Choose two.)
A. Supports the use of PEAP EAP type only.
B. Authenticates users created locally or on a remote LDAP server.
C. Can support the use of a self-sighed or publicly signed certificate for server authentication.
D. FortiGate operates as authentication server only.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 3
When enabling a Security Fabric connection on a FortiGate interface to manage FortiAP devices, which two types of CAPWAP communication channels are established between FortiGate and the FortiAP devices? (Choose two.)
A. Control channels
B. Data channels
C. Security channels
D. FortiLink channels
Answer: A,B (LEAVE A REPLY)
FortiAPs and the FortiGate establish two distinct CAPWAP tunnels when you enable the Security Fabric Connection:
- Control channels carry management and configuration traffic (encrypted by DTLS by default) between the FortiGate and each FortiA
- Data channels carry user-plane (client) traffic across the CAPWAP tunnel, separate from the control path

NEW QUESTION: 4
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 (DFS) regulations.
Answer: (SHOW ANSWER)
Channels 52-144 fall within the DFS-required UNII-2 and UNII-2 Extended bands, meaning APs must monitor for radar signals and vacate those frequencies if radar is detected before transmitting.

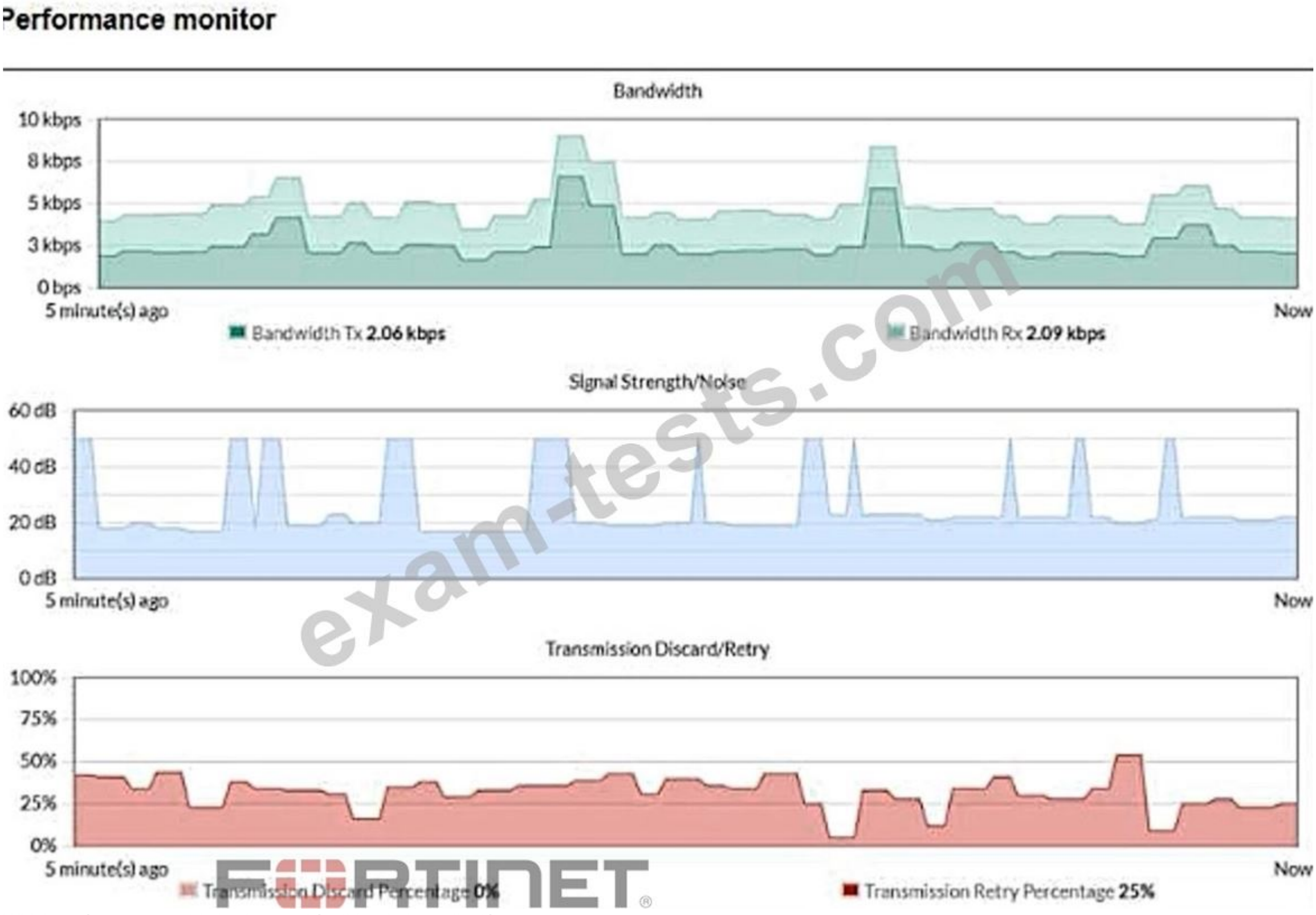
NEW QUESTION: 5
When preauthorizing an AP in the GUI, which minimum configuration parameter is required to add an AP?
A. The AP serial number
B. The AP serial number and FortiAP Profile
C. The FortiAP Profile and AP name
D. The AP serial number, FortiAP Profile, and AP login password
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
A company requires a secure wireless network to span several adjacent buildings. Employees need seamless roaming access across buildings, floors, and, potentially, outdoor areas. FortiAP devices will be used.
Which deployment is the most scalable, manageable, and cost-effective in this scenario?
A. Configure FortiGuard-capable FortiAP devices to broadcast the corporate SSID without being managed by FortiGate in the main building.
B. Deploy a WAN connection on each building to allow FortiAP devices to communicate with FortiGate in the main building.
C. Install FortiWiFi with a cellular modem in the buildings and areas where no wireless signal reaches from the main building.
D. Implement a wireless mesh design to allow FortiAP devices to use neighboring FortiAP devices to connect with FortiGate in the main building.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
You have just authorized a newly added FortiAP device on FortiGate. It went offline for an extended time without coming back online again. What troubleshooting process must you take to bring FortiAP back online?
A. Access FortiAP management using HTTPs.
B. Verify that communication between FortiAP and the wireless controller is not blocked.
C. Restart the wireless controller if it is unresponsive for the newly added FortiAP device.
D. Check the power feed to the FortiAP device and PoE status if powered by a switch.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
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 (LEAVE A REPLY)
A transmission retry rate of around 25 % (one retry in four) is far above normal - indicating roughly that a quarter of all frames must be resent (and many of those may ultimately be dropped), which is an abnormal performance metric for a healthy client connection.

NEW QUESTION: 9
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 (LEAVE A REPLY)
WPA3 replaces the vulnerable four-way WPA2 handshake with SAE (Simultaneous Authentication of Equals), which provides robust forward secrecy and is not susceptible to the KRACK replay-attack flaws that affect WPA2. This ensures each session's keys cannot be recovered or reused by an attacker monitoring handshake messages.

NEW QUESTION: 10
What protection does WPA3 wireless encryption provide over WPA2 for securing wireless networks?
A. WPA3 prevents legacy and deprecated wireless protocols from being used
B. WPA3 uses 128-bit session key size
C. WPA3 enforces only enterprise security mode
D. WPA3 addresses the KRACK vulnerability
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
Which two threats on wireless networks are detected by WIDS? (Choose two.)
A. Brute-force dictionary attacks
B. Unauthorized wireless connection
C. Rogue access points
D. WPA2 authentication vulnerabilities
Answer: A,C (LEAVE A REPLY)
Brute-force dictionary attacks (Asleap)
WIDS includes detection for Asleap attacks - tools that perform brute-force dictionary attacks against LEAP authentication - so you'll see an intrusion alert whenever such a dictionary attack is observed on your air-side traffic Rogue access points WIDS continuously scans for and flags any unauthorized (rogue) APs broadcasting within your RF environment, alerting you the moment a rogue SSID or BSSID appears.

NEW QUESTION: 12
Refer to the exhibits. 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 IoT devices. Users connecting to the guest network located in the reception area are reporting slow performance.

Which configuration change is most likely to improve performance?

AP profile

```
config wireless-controller wtp-profile
    edit "Main networks - 23J"
        config platform
            set type 23JF
            set ddscan enable
        end
        set handoff-sta-thresh 55
        set ap-country SA
        set frequency-handoff enable
        config radio-1
            set band 802.11n-only
            set power-level 50
            set vap-all manual
            set vaps "Contractors" "Guest" "Main-Wifi" "Staff" "Students" "Wifi_IOT" "Wifi_POS"
        end
        config radio-2
            set band 802.11ac-only
            set channel-bonding 40MHz
            set power-level 60
            set vap-all manual
            set vaps "Contractors" "Main-Wifi" "Staff" "Students" "Wifi_IOT" "Wifi_POS"
        end
        config radio-3
            set mode monitor
            set wids-profile "default-wids-apscan-enabled"
        end
    next
end
```

The controller RF analysis output

```
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

Diagnostics and Tools - FP23JFTF211111111

	FP23JFTF211111111
Serial Number	FP23JFTF21001303
Base MAC Address	d4:76:a0:b1:8b:a8
Status	Online
Country/Region	SA
Connected Via	APs / S108FFTV23013917 - port3
IPv4 Address	10.10.0.4
Uptime	13m 11s
Version	v7.4.2 build0634
Registration	Not Registered Register

Actions Edit

General

9% CPU Usage

40% Memory Usage

1.0 Gbps wan

Radio 1 - 2.4 GHz (CH1)

N/A Interfering SSIDs

19 Clients

70% Channel Utilization

Radio 2 - 5 GHz (CH116)

N/A Interfering SSIDs

11 Clients

0% Channel Utilization

Performance | Clients | Interfering SSIDs | WiFi Map | Logs | CLI Access | Spectrum Analysis | VLAN Probe

Refresh | Diagnostics and Tools | Search

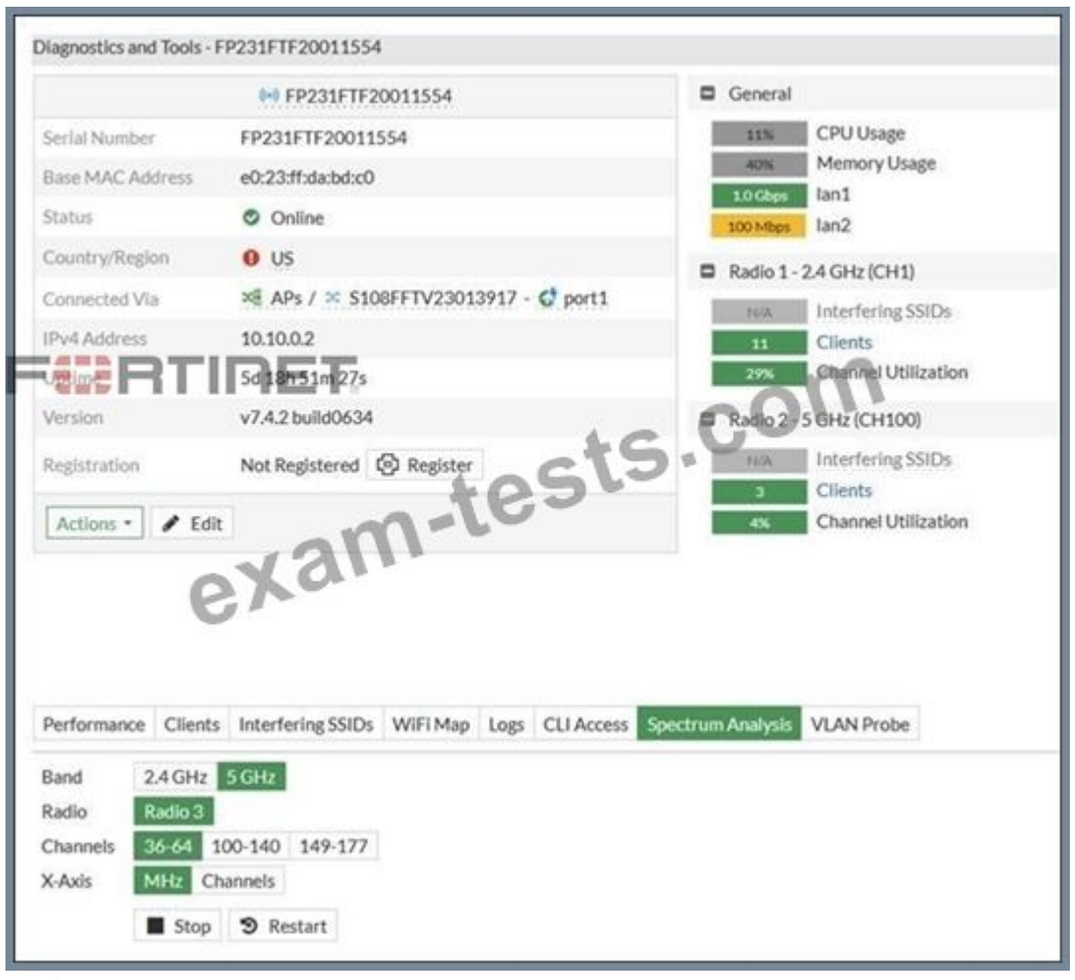
SSID	Device	Channel	Bandwidth Tx/Rx	Signal Strength
Contractors (Contractors)	TECNO-SPARK-7P	1	11.97 kbps	-69 dBm
Contractors (Contractors)	cac28e1:29:cec8	1	0 bps	-70 dBm
Contractors (Contractors)	c4a22f31-d2d9-4b29-9a45-0c017a6b32bb	1	472.07 k...	-76 dBm
Guest (Guest)	wlan0	1	428 bps	-85 dBm
Main-Wifi (Main-Wifi)	WYZEC1-JZ-2CAA8E9C4F99	1	972.45 k...	-76 dBm
Staff (Staff)	Indoorcam-5	1	3.36 kbps	-84 dBm
Contractors (Contractors)	Indoorcam-3	1	3.21 kbps	-70 dBm

Guest (Guest)	Indoorcam-6	1	143.69 k...	-85 dBm
Main-Wifi (Main-Wifi)	Indoorcam	1	5.14 kbps	-75 dBm
Staff (Staff)	Indoorcam-2	1	356.63 k...	-67 dBm
Contractors (Contractors)	Indoorcam-4	1	224.97 k...	-85 dBm
Guest (Guest)	2a:26:3e:24:2f:26	1	9.15 kbps	-75 dBm
Main-Wifi (Main-Wifi)	f7bb8a98-05c5-42b2-836b-29916e7c694b	1	189 bps	-67 dBm
Staff (Staff)	Sullys-14	1	28 bps	-85 dBm
Contractors (Contractors)	78eb2769-1b0b-c0fe-a111-6393b6c8bd59	1	6.05 kbps	-75 dBm
Guest (Guest)	92:ae:c9:6e:01:0a	1	0 bps	-67 dBm

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: (SHOW ANSWER)

Every SSID (VAP) generates its own beacon and management frames, which on a heavily- utilized 2.4 GHz channel (91 % busy) adds significant overhead and cuts into airtime for client data. By cutting back to only the SSIDs needed in the reception area (for example, Guest and perhaps one additional SSID), you'll reduce beacon traffic and free up more of that already- scarce airtime for user throughput.

NEW QUESTION: 13
Refer to the exhibit. Why is Radio 3 used for the spectrum analysis?



A. Only Radio 3 is compatible with the selected band.

B. The 5 GHz frequency band is available only on Radio 3.

C. Radio 1 and Radio 2 are unavailable to run the spectrum analysis.

D. Radio 3 is the configured dedicated monitoring radio for this FortiAP model.

Answer: D (LEAVE A REPLY)