

Fortinet

NSE5_FWF_AD-7.6

Fortinet NSE 5 - Secure Wireless LAN 7.6 Administrator

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/nse5-fwf-ad-7-6>

Latest Version: 6.1

Question: 1

An administrator is trying to confirm whether a wireless issue affects one device type or many. Which source should be reviewed first?

Response:

- A. Client information
- B. Firewall policy list
- C. LED behavior
- D. Cable labels

Answer: A

Explanation:

Reviewing client information reveals whether a problem affects one device type or many.

Question: 2

Which two statements are true about AP profiles?

(Choose two.)

Response:

- A. AP profiles are model specific.
- B. A profile must be applied manually to an AP before it can be managed by FortiGate.
- C. An AP must be authorized before having a profile applied.
- D. A FortiAP profile must be applied to a FortiAP group.

Answer: A,C

Explanation:

FortiAP profiles are tied to a specific AP model because radio and hardware capabilities differ per platform.

A FortiAP must be discovered and authorized on the FortiGate before a profile takes effect.

Question: 3

When configuring a wireless network for dynamic VLAN allocation, which three IETF attributes must be supplied by the RADIUS server?

(Choose three.)

Response:

- A. 81 Tunnel-Private-Group-ID
- B. 65 Tunnel-Medium-Type
- C. 83 Tunnel-Preference
- D. 58 Egress-VLAN-Name
- E. 64 Tunnel-Type

Answer: B,C,E

Explanation:

Tunnel-Private-Group-ID carries the VLAN ID that the RADIUS server returns for dynamic assignment. Tunnel-Medium-Type identifies the transport medium (IEEE 802) and is one of the three required attributes.

Tunnel-Type must be set to VLAN so the RADIUS server signals that a VLAN is being assigned.

Question: 4

An administrator is comparing the behavior of a healthy client and a failing client on the same WLAN. Which objective is most directly involved?

Response:

- A. Interpret client data
- B. Build guest portals
- C. Configure AIOps
- D. Tune radio power

Answer: A

Explanation:

Comparing a healthy and a failing client is an exercise in interpreting client data.

Question: 5

Match each management objective to the best Fortinet mechanism.

- A) Apply the same radio settings to many APs
 - B) Control FortiAP devices centrally
 - C) Evaluate movement and presence trends
 - D) Assist with operational issue insight
- Select the option that maps every objective correctly.

Response:

- A. A → Custom access point profile B → FortiGate integrated wireless controller C → FortiPresence D → FortiAIOps
- B. A → FortiPresence B → FortiGate integrated wireless controller C → Custom access point profile D → FortiAIOps
- C. A → Custom access point profile B → FortiAIOps C → FortiPresence D → FortiGate integrated wireless controller

D. A → Custom access point profile B → FortiGate integrated wireless controller C → FortiAI Ops D → FortiPresence

Answer: A

Explanation:

This option pairs every objective with the correct mechanism: profiles for shared radio settings, FortiGate as controller, FortiPresence for movement trends, and FortiAI Ops for operational insight.

Question: 6

An AP team wants to balance service delivery and security visibility by scanning selected channels instead of every possible one.

Why is this approach useful?

Response:

- A. It reduces the number of channels scanned and can improve the reporting interval
- B. It removes the need for WIDS profiles entirely
- C. It eliminates the need for AP monitoring radios
- D. It guarantees all rogue APs are suppressed automatically

Answer: A

Explanation:

Scanning selected channels lowers scanning overhead and can shorten the reporting interval.

Question: 7

An administrator wants to apply the same radio, channel, and SSID settings to multiple FortiAP devices at once. Which method is the most appropriate?

Response:

- A. Use a custom access point profile
- B. Create one SSID per FortiAP manually
- C. Configure each radio through CLI only
- D. Use FortiPresence location groups

Answer: A

Explanation:

A custom access point profile applies the same radio, channel, and SSID settings to many FortiAPs at once.

Question: 8

A wireless client population includes voice handsets, laptops, and IoT sensors.
Why should the administrator understand wireless technology standards before creating SSIDs?
Response:

- A. Different client types may support different capabilities and performance levels
- B. Standards only matter when using FortiAnalyzer reports
- C. SSIDs are unrelated to radio capability planning
- D. Standards remove the need to tune AP profiles

Answer: A

Explanation:

Because client types vary in the standards and capabilities they support, understanding those standards guides sound SSID and radio planning.

Question: 9

Which two statements about wireless NAC support are correct?
(Choose two.)
Response:

- A. Wireless NAC can onboard clients into a default VLAN
- B. NAC policies can match clients by device properties, user groups, or EMS tags
- C. Wireless NAC works only for wired FortiSwitch ports
- D. Wireless NAC cannot assign clients to specific VLANs
- E. Wireless NAC replaces SSID configuration entirely

Answer: A,B

Explanation:

New devices can be placed onto a default onboarding VLAN until a NAC policy moves them to their assigned segment.

Wireless NAC policies can match on device attributes, user group membership, or FortiClient EMS tags to decide placement.

Question: 10

Refer to the exhibit.

Diagnostics and Tools - FP231FTF20011554

FP231FTF20011554	
Serial Number	FP231FTF20011554
Base MAC Address	e0:23:ff:da:bd:c0
Status	✔ Online
Country/Region	! US
Connected Via	✕ APs / ✕ S108FFTV23013917 - 🌐 port1
IPv4 Address	10.10.0.2
Uptime	5d 18h 51m 27s
Version	v7.4.2 build0634
Registration	Not Registered Register
Actions ▾ Edit	

General

- 11% CPU Usage
- 40% Memory Usage
- 1.0 Gbps lan1
- 100 Mbps lan2

Radio 1 - 2.4 GHz (CH1)

- N/A Interfering SSIDs
- 11 Clients
- 29% Channel Utilization

Radio 2 - 5 GHz (CH100)

- N/A Interfering SSIDs
- 3 Clients
- 4% Channel Utilization

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

Band

2.4 GHz
5 GHz

Radio

Radio 3

Channels

36-64
100-140
149-177

X-Axis

MHz
Channels

Stop
 Restart

Answer: B

Explanation:

The exhibit shows a FortiAP with three radios, and the Spectrum Analysis tool runs on Radio 3 because that radio is the dedicated monitoring/scanning radio on this model, leaving Radio 1 (2.4 GHz) and Radio 2 (5 GHz) to serve clients.

Question: 11

Two APs are located in a shop that is required to support forty 2.4 GHz point-of-sale wireless devices. The APs are managed by a centrally hosted FortiGate. A previous wireless network administrator has enabled client load balancing between APs.

However, the clients are not balancing well between the APs, causing overloading on one of the AP radios. Refer to the exhibit, which is part of the configuration of the AP profile that is used for the APs.

```
# show full-configuration wireless-controller wtp-profile
Shop
config wireless-controller wtp-profile
  edit "Shop"
    set comment "Profile with standard networks"
    config platform
      set type 320C
    end
    set dtls-policy clear-text
    set max-clients 0
    set handoff-rssi 30
    set handoff-sta-thresh 10
    set handoff-roaming enable
    set ap-country GB
    set ip-fragment-preventing tcp-mss-adjust
    config radio-1
      set mode ap
      set band 802.11n,g-only
      set protection-mode disable
      unset powersave-optimize
      set amsdu enable
      set coexistence enable
      set short-guard-interval disable
      set channel-bonding 20MHz
      set auto-power-level disable
      set channel-utilization enable
      set spectrum-analysis disable
      set wids-profile "default-wids-apscan-enabled"
      set darrp enable
      set max-clients 0
      set max-distance 0
      set frequency-handoff disable
      set ap-handoff enable
      set channel "1" "6" "11"
      set vap-all disable
      set vaps "POG"
      set call-admission-control disable
    end
    config radio-2
      set mode ap
      set band 802.11ac
      unset powersave-optimize
      set short-guard-interval disable
      set channel-bonding 40MHz
      set auto-power-level disable
      set power-level 100
    end
  end
end
set dtim 1
set wids-profile "default-wids-apscan-enabled"
set darrp enable
set max-clients 0
set max-distance 0
set frequency-handoff disable
set ap-handoff enable
set vap-all disable
set vaps "POG"
set channel "36" "44" "52"
set call-admission-control disable
```

The first AP has 35 clients associated with it, the second has five clients associated with it. The detected noise floor of the network is -91 dBm. The channel utilization for both 2.4 GHz interfaces is less than 40%. The clients have a detected signal strength of between -53 and -71 dBm.

Which configuration change would improve the distribution of wireless clients between the APs?

Response:

- A. Manually configure 2.4 GHz interfaces of both APs to separate channels.
- B. Increase the handoff-sta-thresh option to 20.
- C. Set the max-clients option to 20.
- D. Decrease the handoff-rssi option to 20.

Answer: D

Explanation:

The exhibit shows the profile with handoff-rssi set to 30 while the clients report signal strengths of -53 to -71 dBm; because channel utilization is low and noise is not a factor, adjusting handoff-rssi to 20 lets the load-balancing handoff act on these clients so the overloaded AP can redistribute them to the underused AP.

Question: 12

Refer to the exhibit.

Radio 2

Mode: ☐ Disabled ☒ Access Point ☐ Dedicated Monitor

WIDS profile: ☒ default-wids-apscan-enabled ▼

Radio resource provision: ☐

Band: 5 GHz 802.11ac/n/a ▼

Channel width: ☒ 20MHz ☐ 40MHz ☐ 80MHz

Short guard interval: ☐

Channels:

☒ 36	☒ 40	☒ 44
☒ 48	☒ 52*	☒ 56*
☒ 60*	☒ 64*	☒ 100*
☒ 104*	☒ 108*	☒ 112*
☒ 116*	☒ 120*	☒ 124*
☒ 128*	☒ 132*	☒ 136*
☒ 140*	☒ 144*	☒ 149
☒ 153	☒ 157	☒ 161
☒ 165		

TX power control: ☒ Auto ☐ Manual

TX power: — dBm

SSIDs: ☒ ((.)) Tunnel ☐ Bridge ☐ Manual

Monitor channel utilization: ☐

What does the asterisk (*) symbol beside the channel mean?

- A. Indicates channels that are subject to dynamic frequency selection (DFS) regulations
- B. Indicates channels that cannot be used because of regulatory channel restrictions
- C. Indicates channels that will be scanned by the Wireless Intrusion Detection System (WIDS)
- D. Indicates channels that can be used only when Radio Resource Provisioning is enabled

Answer: A

Explanation:

In the exhibit the asterisk appears on the 5 GHz channels from 52 through 144; these are DFS channels, where the AP must monitor for radar and vacate the channel if radar is detected.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>