



# NSE6\_FWF-6.4<sup>Q&As</sup>

Fortinet NSE 6 - Secure Wireless LAN 6.4

## Pass Fortinet NSE6\_FWF-6.4 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

[https://www.passapply.com/nse6\\_fwf-6-4.html](https://www.passapply.com/nse6_fwf-6-4.html)

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





### QUESTION 1

Which statement is correct about security profiles on FortiAP devices?

- A. Security profiles can only be applied to unencrypted wireless traffic.
- B. Security profiles can only be applied via firewall policies on the FortiGate.
- C. Security profiles are only supported on Bridge-mode SSIDs.
- D. Security profiles on FortiAP devices can use FortiGate subscription to inspect the traffic.

Correct Answer: D

Security profiles on FortiAP devices can use FortiGate subscription to inspect the traffic, such as antivirus, web filtering, application control, and IPS. This feature is called local bridging and it allows the FortiAP to forward traffic to the FortiGate for security inspection before sending it to the destination network. This reduces the bandwidth consumption and latency of tunnel mode SSIDs. References: Secure Wireless LAN Course Description, page 9; [FortiOS 6.4.0 Handbook - Wireless Controller], page 46.

---

### QUESTION 2

Refer to the exhibits. Exhibit A.



```
config wireless-controller wtp-profile
  edit "Main Networks - FAP-320C"
    set comment "Profile with standard networks"
    config platform
      set type 320C
    end
    set handoff-rssi 30
    set handoff-sta-thresh 30
    set ap-country GB
    config radio-1
      set band 802.11n
      set power-level 50
      set channel-utilization enable
      set wids-profile "default-wids-apscan-enabled"
      set darrp enable
      set vap-all manual
      set vaps "Main-Wifi" "Contractors" "Guest"
      "Wifi_IOT" "Wifi_POS" "Staff" "Students"
      set channel "1" "6" "11"
    end
    config radio-2
      set band 802.11ac
      set channel-bonding 40MHz
      set power-level 60
      set channel-utilization enable
      set wids-profile "default-wids-apscan-enabled"
      set darrp enable
      set vap-all manual
      set vaps "Main-Wifi" "Contractors" "Guest"
      "Wifi_IOT" "Wifi_POS" "Staff" "Students"
      set channel "36" "44" "52" "60"
    end
  end
next
end
```

Exhibit B.



Diagnostics and Tools - Office

Office	
Serial Number	FPXXXXXXXXXXXX
Base MAC Address	xx:xx:xx:xx:xx:xx
Status	<span style="color: green;">✔</span> Online
Country/Region	GB
Uplink Interface	FortiAP management (ap)
IPv4 Address	192.168.5.98
Uptime	12m1s
Version	v6.4 build0437

General

56%	CPU Usage
70%	Memory Usage
0 days	Connection Uptime
1.0 Gbps	lan1
0 Mbps	lan2

Radio 1 - 2.4 GHz

31	Interfering SSIDs
1	Clients
25%	Channel Utilization

Radio 2 - 5 GHz

0	Interfering SSIDs
30	Clients
5%	Channel Utilization

- Radios
Clients
Interfering SSIDs
Logs
CLI Access
Spectrum Analysis
VLAN Probe

	Radio 1 - 2.4 GHz	Radio 2 - 5 GHz
Mode	AP	AP
SSID	AP fortinet (Main-WiFi) AP fortinet2 (Contractors) AP fortinet3 (Guest)	AP fortinet (Main-WiFi) AP fortinet2 (Contractors) AP fortinet3 (Guest)
Clients	1	20
Bandwidth Tx	4.65 kbps	1.16 kbps
Bandwidth Rx	20.46 kbps	176 bps
Operating Channel	1	60
Channels		
Operating TX Power	3 dBm	21 dBm
Band	802.11n	802.11ac

Interfering SSIDs for Office (Radio 1) x

SSID	AP BSSID	Channel	Signal
Husky	aa:aa:aa:aa:aa	1	-84 dBm
Husky guest	bb:bb:bb:bb:bb	1	-84 dBm
KBANK5007	cc:cc:cc:cc:cc	1	-85 dBm
mandikaylee	dd:dd:dd:dd:dd	1	-86 dBm
	ee:ee:ee:ee:ee	1	-87 dBm
HUAWEI-EMIX4f	ee:ee:ee:ee:ef	1	-88 dBm
trojan-3	ff:ff:ff:ff:ff	1	-88 dBm
	fg:gg:gg:gg:gg	1	-89 dBm
	hg:gg:gg:gg:gg	1	-89 dBm

Exhibit C.



```
# get wireless-controller rf-analysis FPXXXXXXXXXXXXXXXXX
WTP: Office 0 192.168.5.98:5246
```

channel	rssi-total	rf-score	overlap-ap	interfere-ap	chan-utilization
1	100	6	13	13	63%
2	23	10	0	22	47%
3	15	10	0	22	15%
4	24	10	0	22	15%
5	51	10	0	22	41%
6	223	1	9	9	75%
7	52	10	0	17	47%
8	32	10	0	17	13%
9	27	10	0	19	10%
10	45	10	0	19	28%
11	177	1	8	10	65%
12	46	10	0	10	34%
13	45	10	2	10	70%
14	14	10	0	10	0%
36	16	10	2	2	0%
44	83	7	5	5	0%

A wireless network has been installed in a small office building and is being used by a business to connect its wireless clients. The 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. The network administrator is reviewing the information shown in the exhibits as part of the ongoing investigation of the problem. They show the profile used for the AP and the controller RF analysis output together with a screenshot of the GUI showing a summary of the AP and its neighboring APs.

To improve performance for the users connecting to the guest network in this area, which configuration change is most likely to improve performance?

- A. Increase the transmission power of the AP radios
- B. Enable frequency handoff on the AP to band steer clients
- C. Reduce the number of wireless networks being broadcast by the AP
- D. Install another AP in the reception area to improve available bandwidth

Correct Answer: A

### QUESTION 3

A tunnel mode wireless network is configured on a FortiGate wireless controller. Which task must be completed before the wireless network can be used?

- A. The wireless network interface must be assigned a Layer 3 address



- B. Security Fabric and HTTPS must be enabled on the wireless network interface
- C. The wireless network to Internet firewall policy must be configured
- D. The new network must be manually assigned to a FortiAP profile

Correct Answer: C

A FortiGate unit is an industry leading enterprise firewall. In addition to consolidating all the functions of a network firewall, IPS, anti-malware, VPN, WAN optimization, Web filtering, and application control in a single platform, FortiGate also has an integrated Wi-Fi controller.

Reference: [https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/723e20ad-5098-11e9-94bf-00505692583a/FortiWiFi\\_and\\_FortiAP-6.2.0-Configuration\\_Guide.pdf](https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/723e20ad-5098-11e9-94bf-00505692583a/FortiWiFi_and_FortiAP-6.2.0-Configuration_Guide.pdf)

---

#### QUESTION 4

As standard best practice, which configuration should be performed before configuring FortiAPs using a FortiGate wireless controller?

- A. Create wireless LAN specific policies
- B. Preauthorize APs
- C. Create a custom AP profile
- D. Set the wireless controller country setting

Correct Answer: C

Reference: <https://docs.fortinet.com/document/fortiap/6.4.1/fortiwifi-and-fortiap-configuration-guide/547298/complex-wireless-network-example>

---

#### QUESTION 5

How are wireless clients assigned to a dynamic VLAN configured for hash mode?

- A. Using the current number of wireless clients connected to the SSID and the number of IPs available in the least busy VLAN
- B. Using the current number of wireless clients connected to the SSID and the number of clients allocated to each of the VLANs
- C. Using the current number of wireless clients connected to the SSID and the number of VLANs available in the pool
- D. Using the current number of wireless clients connected to the SSID and the group the FortiAP is a member of

Correct Answer: C

VLAN from the VLAN pool based on a hash of the current number of SSID clients and the number of entries in the VLAN pool.

Reference: <https://docs.fortinet.com/document/fortiap/7.0.1/fortiwifi-and-fortiap-configuration-guide/376326/configuring->

---



dynamic-user-vlan-assignment

[NSE6\\_FWF-6.4 PDF  
Dumps](#)

[NSE6\\_FWF-6.4 VCE  
Dumps](#)

[NSE6\\_FWF-6.4 Exam  
Questions](#)