



Download Fortinet FCP_FWF_AD-7.4 Exam Dumps Free

Shared by Huffman on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

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?

Options:

- 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:

A

Question 2

Question Type: MultipleChoice

Refer to the exhibit.



WiFi Settings

WiFi Settings

SSID

Client limit

Broadcast SSID

Beacon advertising Name Model Serial number

Security Mode Settings

Security mode

Authentication

Client MAC Address Filtering

RADIUS server

Address group policy

Additional Settings

Dynamic VLAN assignment

Schedule

Block intra-SSID traffic

Optional VLAN ID

Broadcast suppression

- ARPs for known clients
- DHCP unicast
- DHCP uplink

Quarantine host

VLAN pooling

NAC profile

FortiGate sends logs to FortiAnalyzer using the default settings to report security events for all wireless stations as part of the Security Fabric configuration

Which security action will FortiGate take when it detects a compromised wireless station in the CORP_DATA SSID?

Options:

A- CORP_DATA is in NAC mode and onboards compromised stations for a period until malicious activity stops

- B- FortiGate disassociates compromised stations and prevents them from connecting again
- C- FortiAnalyzer generates security reports to inform security operations to further Investigate the compromised stations
- D- FortiAP devices broadcasting CORP_DATA wireless network place compromised stations in quarantine

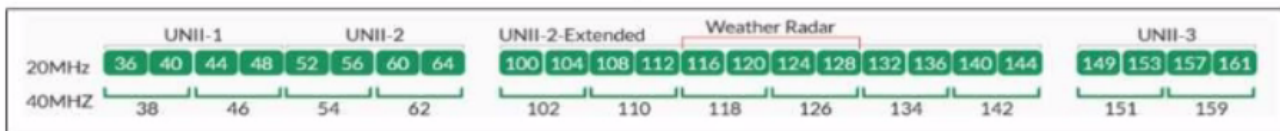
Answer:

A

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



Which statement is correct about channels 52 through 144 in the 5 GHz band?

Options:

- 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:

B

Question 4

Question Type: MultipleChoice

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.)

Options:

- 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:

C, D



Question 5

Question Type: MultipleChoice

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?

Options:

- 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



Question 6

Question Type: MultipleChoice

Refer to the exhibits.

```
61E-01 # get wireless-controller rf-analysis
```

```
WTP: FP23JFTF211111111 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 screenshot displays the 'Diagnostics and Tools' interface for an AP. The top section shows general information for AP ID FP23JFTF211111111. Below this, there are performance metrics for CPU Usage (9%), Memory Usage (4%), and wlan (1.0 Gbps). The interface also shows details for Radio 1 (2.4 GHz) and Radio 2 (5 GHz), including Interfering SSIDs, Clients, and Channel Utilization. A table at the bottom lists neighboring APs with columns for SSID, Device, Channel, Bandwidth Tx/Rx, and Signal Strength.

SSID	Device	Channel	Bandwidth Tx/Rx	Signal Strength
Contractors (Contractors)	TECNO-SPARK-7P	1	11.97 kbps ↓	-69 dBm
Contractors (Contractors)	car20e129xecd	1	0 bps	-70 dBm
Contractors (Contractors)	c4a22f31-d209-4b29-9a45-0c017a6b32bb	1	472.07 k...	-76 dBm
Guest (Guest)	wlan0	1	428 bps ↓	-85 dBm
Main-Wifi (Main-Wifi)	WYZEC1-JZ-2CAABE9CAF99	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)	2a263e242f26	1	9.15 kbps ↓	-75 dBm
Main-Wifi (Main-Wifi)	f71b8a98-05c5-42b2-836b-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)	92aacc96e010a	1	0 bps	-67 dBm

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?

Options:

- 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

Question 7

Question Type: MultipleChoice

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



Options:

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

Answer:

D

Question 8

Question Type: MultipleChoice

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

```

RADIUS configuration

Username:	user1
<input type="checkbox"/> Disabled	
RADIUS Attribute:	
Vendor:	Default
Attribute ID:	Tunnel-Type
Value:	Integer
Type:	Integer
RADIUS Attribute:	
Vendor:	Default
Attribute ID:	Tunnel-Medium-Type
Value:	IEEE-802
Type:	Integer
RADIUS Attribute:	
Vendor:	Default
Attribute ID:	Tunnel-Private-Group-Id
Value:	infrastructure
Type:	String
<input type="button" value="+ Add RADIUS Attribute"/>	

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?

Options:

- 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

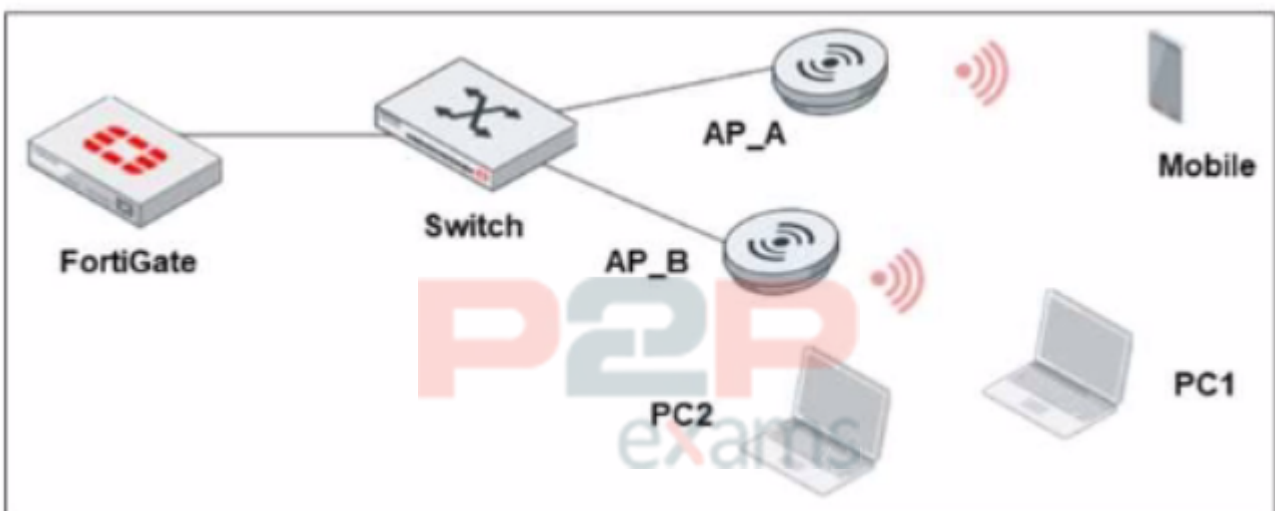
Answer:

C

Question 9

Question Type: MultipleChoice

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?

Options:

- 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



To Get Premium Files for FCP_FWF_AD-7.4
Visit

https://www.p2pexams.com/products/fcp_fwf_ad-7.4

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/fcp-fwf-ad-7.4>

20%
DISCOUNT

P2P
exams