

NSE6_FWF-6.4^{Q&As}

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.pass2lead.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

Refer to the exhibits.

Exhibit A Exhibit B

```
53836.574 xx:xx:xx:xx:xx:xx <ih> IEEE 802.11 mgmt::assoc_req <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rId 1 wId2
yy:yy:yy:yy:yy:yy

53836.574 xx:xx:xx:xx:xx:xx <ih> xx:xx:xx:xx:xx:xx sta =
0x6311c88, sta->flags = 0x00000001, auth_alg = 0, hapd->splitMac: 1

53836.575 xx:xx:xx:xx:xx:xx <ih> IEEE 802.11 mgmt::assoc_resp <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rId 1 wId2
yy:yy:yy:yy:yy:yy

53836.575 xx:xx:xx:xx:xx:xx <ih> IEEE 802.11 mgmt::assoc_resp <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rId 1 wId2
yy:yy:yy:yy:yy:yy

53836.575 xx:xx:xx:xx:xx:xx <dc> STA add xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId2 bssid
yy:yy:yy:yy:yy:yy NON-AUTH band 0x10 mimo 2*2

53836.575 xx:xx:xx:xx:xx:xx <cc> STA_CFG_REQ(10) sta
xx:xx:xx:xx:xx:xx add ==> ws (0-192.168.5.98:5246) rId 1 wId 2

53836.576 xx:xx:xx:xx:xx:xx <cc> STA add xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId 2 yy:yy:yy:yy:yy:yy sec
WPA2 PERSONAL auth 0

53836.576 xx:xx:xx:xx:xx:xx cwAcStaRbtAdd: I2C_STA_ADD insert sta
xx:xx:xx:xx:xx:xx 192.168.5.98/1/2/1

53836.577 xx:xx:xx:xx:xx:xx <cc> STA_CFG_RESP(10) sta xx:xx:xx:xx:xx:xx
<== ws (0-192.168.5.98:5246) rc 0 (Success)

64318.579 xx:xx:xx:xx:xx:xx <eh> RADIUS message (type=0) ==> RADIUS
Server code=1 (Access-Request) id=9 len=214

64318.579 xx:xx:xx:xx:xx:xx <eh> send 1/4 msg of 4-Way
Handshake

64318.580 xx:xx:xx:xx:xx:xx <eh> send IEEE 802.1X ver=2 type=3
(EAPOL_KEY) data len=95 replay cnt 1

64813.580 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL99B) ==>
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId 2
yy:yy:yy:yy:yy:yy

64318.582 xx:xx:xx:xx:xx:xx <eh> RADIUS message (type=0) <== RADIUS
Server code=2 (Access-Accept) id=9 len=114

53836.582 xx:xx:xx:xx:xx:xx <dc> STA chg xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId 2 bssid
yy:yy:yy:yy:yy:yy Auth:allow
```

```
64813.583 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 121B) <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.583 xx:xx:xx:xx:xx:xx <eh>      recv IEEE 802.1X ver=1 type=3
(EAPOL_KEY) data len=117

64813.583 xx:xx:xx:xx:xx:xx <eh>      recv EAPOL-Key 2/4 Pairwise
replay cnt 1

64813.583 xx:xx:xx:xx:xx:xx <eh>      send 3/4 msg of 4-Way
Handshake

64813.584 xx:xx:xx:xx:xx:xx <eh>      send IEEE 802.1X ver=2 type=3
(EAPOL_KEY) data len=151 replay cnt 2

64813.584 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 155B) ==>
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.586 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 99B) <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.586 xx:xx:xx:xx:xx:xx <eh>      recv IEEE 802.1X ver=1 type=3
(EAPOL_KEY) data len=35

64813.586 xx:xx:xx:xx:xx:xx <eh>      recv EAPOL-Key 4/4 Pairwise
replay cnt 2

53836.587 xx:xx:xx:xx:xx:xx <dc> STA chg xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId2 bssid
yy:yy:yy:yy:yy:yy AUTH

53836.587 xx:xx:xx:xx:xx:xx <cc> STA chg xx:xx:xx:xx:xx:xx vap
Wireless ws (0-192.168.5.98:5246) rId 1 wId2 yy:yy:yy:yy:yy:yy sec
WPA2 PERSONAL auth 1 *****

53836.587 xx:xx:xx:xx:xx:xx <cc> STA_CFG_REQ(12) sta
xx:xx:xx:xx:xx:xx add key (len=16) ==> ws (0-192.168.5.98:5246) rId
1 wId2

53836.589 xx:xx:xx:xx:xx:xx <cc> STA_CFG_REQ(12) xx:xx:xx:xx:xx:xx
<== ws (0-192.168.5.98:5246) rc 0 (Success)

53837.140 xx:xx:xx:xx:xx:xx <dc> DHCP Request server 0.0.0.0 <==
host DESKTOP-CVKGHH mac xx:xx:xx:xx:xx:xx ip 192.168.30.2 xId
88548005

53837.142 xx:xx:xx:xx:xx:xx <dc> DHCP Ack server 192.168.30.1 ==>
host mac xx:xx:xx:xx:xx:xx ip 192.168.30.2 mask 255.255.255.0 gw
192.168.30.1 xId 88548005
```

The exhibits show the diagnose debug log of a station connection taken on the controller CLI. Which security mode is used by the wireless connection?

- A. WPA2 Enterprise
- B. WPA3 Enterprise
- C. WPA2 Personal and radius MAC filtering
- D. Open, with radius MAC filtering

Correct Answer: A

Best security option is WPA2-AES.

Reference: <https://www.esecurityplanet.com/trends/the-best-security-for-wireless-networks/>

QUESTION 2

Which two phases are part of the process to plan a wireless design project? (Choose two.)

- A. Project information phase
- B. Hardware selection phase
- C. Site survey phase
- D. Installation phase

Correct Answer: CD

Reference: <https://www.sciencedirect.com/topics/computer-science/wireless-site-survey> <https://www.automation.com/en-us/articles/2015-2/wireless-device-network-planning-and-design>

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-509811e9-94bf-00505692583a/FortiWiFi_and_FortiAP-6.2.0-Configuration_Guide.pdf

QUESTION 4

Six APs are located in a remotely based branch office and are managed by a centrally hosted FortiGate. Multiple wireless users frequently connect and roam between the APs in the remote office.

The network they connect to, is secured with WPA2-PSK. As currently configured, the WAN connection between the branch office and the centrally hosted FortiGate is unreliable.

Which configuration would enable the most reliable wireless connectivity for the remote clients?

- A. Configure a tunnel mode wireless network and enable split tunneling to the local network
- B. Configure a bridge mode wireless network and enable the Local standalone configuration option
- C. Configure a bridge mode wireless network and enable the Local authentication configuration option
- D. Install supported FortiAP and configure a bridge mode wireless network

Correct Answer: A

QUESTION 5

Refer to the exhibits.

Exhibit A

```
config wireless-controller wtp
  edit "FPXXXXXXXXXXXXXXXXX"
    set admin enable
    set name "Authors AP1"
    set wtp-profile "Authors"
    config radio-1
    end
    config radio-2
    end
  next
  edit "FPXXXXXXXXXXXXXXXXYYY"
    set admin enable
    set name " Authors AP2"
    set wtp-profile "Authors"
    config radio-1
    end
    config radio-2
    end
  next
  edit "FPXXXXXXXXXXXXXXXXZZZ"
    set admin enable
    set name " Authors AP3"
    set wtp-profile "Authors"
    config radio-1
    end
    config radio-2
    end
  next
end
```

Exhibit B

```
sh wireless-controller wtp-profile Authors
config wireless-controller wtp-profile
  edit "Authors"
    set comment "APs allocated to authors"
    set handoff-sta-tresh 30
    config radio-1
      set band 802.11n-5G
      set channel-bonding 40MHz
      set auto-power-level enable
      set auto-power-high 12
      set auto-power-low 1
      set vap-all tunnel
      set channel "36" "40" "44" "48" "52" "56"
      "60" "64" "100" "104" "108" "112" "116" "120" "124"
      "128" "132" "136"
    end
    config radio-2
      set band 802.11n, g-only
      set auto-power-level enable
      set auto-power-high 12
      set auto-power-low 1
      set vap-all tunnel
      set channel "1" "6" "11"
    end
  next
end
config wireless-controller vap
  edit "Authors"
    set ssid "Authors"
    set security wpa2-only-enterprise
    set radius-mac-auth enable
    set radius-mac-auth-server "Main AD"
    set local-bridging enable
    set intra-vap-privacy enable
    set schedule "always"
  next
end
```

A wireless network has been created to support a group of users in a specific area of a building. The wireless network is

configured but users are unable to connect to it. The exhibits show the relevant controller configuration for the APs and the wireless network.

Which two configuration changes will resolve the issue? (Choose two.)

- A. For both interfaces in the wtp-profile, configure set vaps to be "Authors"
- B. Disable intra-vap-privacy for the Authors vap-wireless network
- C. For both interfaces in the wtp-profile, configure vap-all to be manual
- D. Increase the transmission power of the AP radio interfaces

Correct Answer: BC

[NSE6_FWF-6.4 Practice Test](#)

[NSE6_FWF-6.4 Exam Questions](#)

[NSE6_FWF-6.4 Braindumps](#)