# 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.geekcert.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**

When enabling security fabric on the FortiGate interface to manage FortiAPs, which two types of communication channels are established between FortiGate and FortiAPs? (Choose two.)

A. Control channels

B. Security channels

C. FortLink channels

D. Data channels

Correct Answer: AD

The control channel for managing traffic, which is always encrypted by DTLS. l The data channel for carrying client data packets.

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ac61f4d3-ce67-11e9-8977-005056 92583a/FortiWiFi_and_FortiAP-6.2-Cookbook.pdf

**QUESTION 3**

Which administrative access method must be enabled on a FortiGate interface to allow APs to connect and function?

A. Security Fabric

B. SSH

C. HTTPS

D. FortiTelemetry

Correct Answer: A

Reference: https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/788897/configuring-the-root-fortigate-and-downstream-fortigates

QUESTION 4

When deploying a wireless network that is authenticated using EAP PEAP, which two configurations are required? (Choose two.)

A. An X.509 certificate to authenticate the client

B. An X.509 to authenticate the authentication server

C. A WPA2 or WPA3 personal wireless network

D. A WPA2 or WPA3 Enterprise wireless network

Correct Answer: AB

X.509 certificates and work for connections that use Secure Socket Layer/Transport Level Security (SSL/TLS). Both client and server certificates have additional requirements. Reference: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-manage-cert-requirements

QUESTION 5

Which factor is the best indicator of wireless client connection quality?

A. Downstream link rate, the connection rate for the AP to the client

B. The receive signal strength (RSS) of the client at the AP

C. Upstream link rate, the connection rate for the client to the AP

D. The channel utilization of the channel the client is using

Correct Answer: B

SSI, or "Received Signal Strength Indicator," is a measurement of how well your device can hear a signal from an access point or router. It\\'s a value that is useful for determining if you have enough signal to get a good wireless connection. Reference: https://www.metageek.com/training/resources/understanding-rssi.html

[NSE6_FWF-6.4 PDF Dumps](#)       [NSE6_FWF-6.4 VCE Dumps](#)       [NSE6_FWF-6.4 Braindumps](#)