PassQueen
a.k.a dumpsqueen.com

Fortinet NSE 6 - Secure Wireless LAN 6.4

Fortinet NSE6_FWF-6.4

Version Demo

Total Demo Questions: 5

Total Premium Questions: 50

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, FortiAP deployment	8
Topic 2, FortiAP management	13
Topic 3, Wireless network configuration	11
Topic 4, Wireless security	7
Topic 5, Wireless authentication	6
Topic 6, Troubleshooting wireless networks	5
Total	50

QUESTION NO: 1

When configuring Auto TX Power control on an AP radio, which two statements best describe how the radio responds? (Choose two.)

A. When the AP detects any other wireless signal stronger that -70 dBm, it will reduce its transmission power until it reaches the minimum configured TX power limit.

B. When the AP detects PF Interference from an unknown source such as a cordless phone with a signal stronger that -70 dBm, it will increase its transmission power until it reaches the maximum configured TX power limit.

C. When the AP detects any wireless client signal weaker than -70 dBm, it will increase its transmission power until it reaches the maximum configured TX power limit.

D. When the AP detects any interference from a trusted neighboring AP stronger that -70 dBm, it will reduce its transmission power until it reaches the minimum configured TX power limit.

ANSWER: A C

Explanation:

Auto TX Power Control dynamically adjusts an access point radio's transmit level according to the RF environment and associated client coverage. When the radio detects another wireless signal stronger than −70 dBm, reducing transmit power helps limit excessive cell overlap and co-channel contention. The radio continues reducing power only to the configured minimum TX-power boundary, ensuring that automatic adjustments remain within the administrator's planned RF limits.

Conversely, a wireless client heard at a level weaker than −70 dBm can indicate that the client is at the edge of usable coverage. In that situation, the access point increases its transmit power, up to the configured maximum TX-power limit, to improve the downstream signal available to that client. These opposing actions support a balanced WLAN design: radios avoid using more power than necessary in dense coverage areas while still extending service where client signal conditions indicate weaker coverage.

Fortinet documents radio transmit-power configuration and automatic power management as part of FortiAP radio profile and wireless-controller configuration. See the FortiWiFi and FortiAP Configuration Guide and the FortiOS 6.4 documentation portal.

QUESTION NO: 2

When deploying EAP-TLS authentication for an Enterprise wireless network, which two certificate requirements are applicable? (Choose two.)

A. An X.509 certificate for the authentication server

B. An X.509 certificate for each authenticating client

C. A shared WPA-Personal pre-shared key for every client

D. A captive portal certificate for wireless client authentication

ANSWER: A B

Explanation:

EAP-TLS uses mutual certificate-based authentication. The authentication server requires an X.509 certificate so that the wireless client can validate the server identity while establishing the TLS session. The client also requires its own X.509 certificate to authenticate to the RADIUS server.

This differs from PEAP deployments, which commonly use a server certificate and password-based inner authentication. EAP-TLS does not use a shared WPA-Personal passphrase for client authentication. See the Network Policy Server certificate requirements and the FortiWiFi and FortiAP Configuration Guide.

QUESTION NO: 3

As a network administrator, you are responsible for managing an enterprise secure wireless LAN. The controller is based in the United States, and you have been asked to deploy a number of managed APs in a remote office in Germany.

What is the correct way to ensure that the RF channels and transmission power limits are appropriately configured for the remote APs?

A. Configure the APs individually by overriding the settings in Managed FortiAPs

B. Configure the controller for the correct country code for Germany

C. Clone a suitable FortiAP profile and change the country code settings on the profile

D. Create a new FortiAP profile and change the country code settings on the profile

ANSWER: C

Explanation:

Clone a suitable FortiAP profile and change the country code settings on the profile. A FortiAP profile contains radio configuration that the FortiGate wireless controller applies to managed FortiAPs, including the regulatory country setting. Setting the profile country to Germany causes the controller to use the regulatory domain applicable to Germany for APs assigned to that profile. This ensures that channel availability and permitted transmit-power limits are derived from the correct local regulatory requirements, rather than from the controller's physical location in the United States.

Cloning an existing suitable profile preserves the organization's established SSID, security, radio, and operational settings while allowing the administrator to make a targeted country-code change for the remote-site AP group. The cloned profile can then be assigned to the Germany-based FortiAPs, providing consistent, centrally managed regulatory compliance across the deployment. Fortinet documents FortiAP profile configuration, including radio and country-related settings, in the FortiWiFi and FortiAP Configuration Guide for FortiOS 6.4.

QUESTION NO: 4

A wireless client can associate to an SSID but does not receive an IP address.

Which service must be available to provide the client with its IPv4 addressing information automatically?

A. DNS

B. DHCP

C. NTP

D. RADIUS accounting

ANSWER: B

Explanation:

DHCP is correct because a client normally obtains its IPv4 address, subnet mask, default gateway, DNS server information, and lease details through DHCP after associating with the wireless network.

Successful association only establishes the wireless Layer 2 connection. In tunnel mode, DHCP requests must be permitted from the SSID interface to the DHCP server. In bridge mode, the FortiAP local wired network must provide access to the DHCP service for the assigned client VLAN. See the FortiOS 6.4 Administration Guide.

QUESTION NO: 5

A wireless administrator wants client traffic from a bridge mode SSID to be forwarded locally onto the wired network at the FortiAP location.

Which SSID traffic mode must be configured?

A. Bridge mode

B. Tunnel mode

C. Remote authentication mode

D. Local standalone mode

ANSWER: A

Explanation:

Bridge mode is correct because it forwards wireless client traffic from the FortiAP directly to its local Ethernet network. Client frames do not use the CAPWAP data tunnel to reach the FortiGate wireless controller for normal data forwarding.

This mode is commonly used when local network access is required at a remote site or when WAN bandwidth should not be consumed by tunneled wireless client traffic. The wired network connected to the FortiAP must provide the appropriate VLAN and DHCP connectivity for wireless clients. See the FortiWiFi and FortiAP Configuration Guide.