NSE6_FWF-6.4 Q&As

Fortinet NSE 6 - Secure Wireless LAN 6.4

QUESTION 1

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 2

Which two statements about distributed automatic radio resource provisioning (DARRP) are correct? (Choose two.)

A. DARRP performs continuous spectrum analysis to detect sources of interference. It uses this information to allow the AP to select the optimum channel.

B. DARRP performs measurements of the number of BSSIDs and their signal strength (RSSI). The controller then uses this information to select the optimum channel for the AP.

C. DARRP measurements can be scheduled to occur at specific times.

D. DARRP requires that wireless intrusion detection (WIDS) be enabled to detect neighboring devices.

Correct Answer: AD

DARRP (Distributed Automatic Radio Resource Provisioning) technology ensures the wireless infrastructure is always optimized to deliver maximum performance. Fortinet APs enabled with this advanced feature continuously monitor the RF environment for interference, noise and signals from neighboring APs, enabling the FortiGate WLAN Controller to determine the optimal RF power levels for each AP on the network. When a new AP is provisioned, DARRP also ensures that it chooses the optimal channel, without administrator intervention.

Reference: http://www.corex.at/Produktinfos/FortiOS_Wireless.pdf

QUESTION 3

Which of the following is a requirement to generate analytic reports using on-site FortiPresence deployment?

A. SQL services must be running

B. Two wireless APs must be sending data

C. DTLS encryption on wireless traffic must be turned off

D. Wireless network security must be set to open

Correct Answer: B

FortiPresence VM is deployed locally on your site and consists of two virtual machines. All the analytics data collected and computed resides locally on the VMs.

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/30bd9962-44e8-11eb-b9ad-00505692583a/FortiPresence_VM-1.0.0-Administration_Guide.pdf

QUESTION 4

Which statement is correct about security profiles on FortiAP devices?

A. Security profiles on FortiAP devices can use FortiGate subscription to inspect the traffic

B. Only bridge mode SSIDs can apply the security profiles

C. Disable DTLS on FortiAP

D. FortiGate performs inspection the wireless traffic

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortiap/6.4.0/fortiwifi-and-fortiap-configuration-guide/47321/fortiap-s-bridge-mode-security-profiles

QUESTION 5

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.