Vendor: Fortinet

Exam Code: NSE6_FWF-6.4

Exam Name: Fortinet NSE 6 - Secure Wireless LAN 6.4

Version: DEMO

QUESTION 1
What type of design model does FortiPlanner use in wireless design project?

A. Architectural model
B. Predictive model
C. Analytical model
D. Integration model

Answer: B
Explanation:
FortiPlanner uses a predictive model to simulate the behavior of wireless networks. This allows users to predict how a network will perform under different conditions, such as the number of users, the type of devices, and the environment.

QUESTION 2
Which two roles does FortiPresence analytics assist in generating presence reports? (Choose two.)

A. Gathering details about on site visitors
B. Predicting the number of guest users visiting on-site
C. Comparing current data with historical records
D. Reporting potential threats by guests on site

Answer: AC
Explanation:
FortiPresence analytics is a cloud-based analytics platform that helps businesses understand how visitors interact with their physical spaces. It does this by collecting data from FortiAP access points, which are deployed at the business's physical locations.
FortiPresence analytics can be used to generate presence reports, which provide insights into how visitors are using the business's space. These reports can be used to improve the customer experience, increase sales, and make better decisions about how to allocate resources.
The two roles that FortiPresence analytics assist in generating presence reports are:
1. Gathering details about on site visitors: FortiPresence analytics collects data about visitors, including their device information, location, and time spent in the business's space. This data can be used to create reports that show how many visitors are coming to the business, where they are coming from, and how long they are staying.
2. Comparing current data with historical records: FortiPresence analytics can also be used to compare current data with historical records. This can be used to identify trends in visitor behavior, such as which days of the week are busiest or which times of day are most popular. This information can be used to make better decisions about how to allocate resources, such as staffing levels and marketing campaigns.

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.

Answer: A
Explanation:
You need to configure DHCP on wireless interface for clients to get IPs, without policies clients can still connect to network but no Internet access.

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

Answer: B
Explanation:
If bridge mode SSID is configured for a managed FortiAP, you can add a security profile feature. This is only support in bridge mode. The traffic of a tunneled SSID is inspected by Fortigate.

QUESTION 5
How are wireless clients assigned to a dynamic VLAN configured for hash mode?

A. Using the current number of wireless clients connected to the SSID and the number of IPs available in the least busy VLAN
B. Using the current number of wireless clients connected to the SSID and the number of clients allocated to each of the VLANs
C. Using the current number of wireless clients connected to the SSID and the number of VLANs available in the pool
D. Using the current number of wireless clients connected to the SSID and the group the FortiAP is a member of

Answer: C
Explanation:
VLAN from the VLAN pool based on a hash of the current number of SSID clients and the number of entries in the VLAN pool.

QUESTION 6
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.

Answer: BC
Explanation:
"When using DARRP, the AP selects the best channel available to use based on the scan results of BSSID/receive signal strength (RSSI) to AC" and "To set the running time for DARRP

optimization, use the following CLI command within the wireless controller setting: set darrp-optimize {integer}. Note that DARRP doesn't do continuous spectrum analysis..."

QUESTION 7
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

Answer: B
Explanation:
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

QUESTION 8
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 reduce 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: AD
Explanation:
When Auto TX Power control is enabled on an AP radio, the AP will automatically adjust its transmission power based on the signal strength of other APs and wireless clients in the area.
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. This is because the AP does not want to over-transmit and cause interference with other APs or wireless clients.
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. This is because the AP does not want to over-transmit and cause interference with its neighboring APs.

QUESTION 9
When configuring a wireless network for dynamic VLAN allocation, which three IETF attributes must be supplied by the radius server? (Choose three.)

A. 81 Tunnel-Private-Group-ID
B. 65 Tunnel-Medium-Type
C. 83 Tunnel-Preference
D. 58 Egress-VLAN-Name

E. 64 Tunnel-Type

Answer: ABE
Explanation:
The RADIUS user attributes used for the VLAN ID assignment are:
IETF 64 (Tunnel Type)--Set this to VLAN.
IETF 65 (Tunnel Medium Type)--Set this to 802
IETF 81 (Tunnel Private Group ID)--Set this to VLAN ID.
Reference: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-vlan/71683-dynamicvlan-config.html

QUESTION 10
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

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

QUESTION 11
You are investigating a wireless performance issue and you are trying to audit the neighboring APs in the PF environment. You review the Rogue APs widget on the GUI but it is empty, despite the known presence of other APs.

Which configuration change will allow neighboring APs to be successfully detected?

A. Enable Locate WiFi clients when not connected in the relevant AP profiles.
B. Enable Monitor channel utilization on the relevant AP profiles.
C. Ensure that all allowed channels are enabled for the AP radios.
D. Enable Radio resource provisioning on the relevant AP profiles.

Answer: D
Explanation:
The ARRP (Automatic Radio Resource Provisioning) profile improves upon DARRP (Distributed Automatic Radio Resource Provisioning) by allowing more factors to be considered to optimize channel selection among FortiAPs. DARRP uses the neighbor APs channels and signal strength collected from the background scan for channel selection.
Reference: https://docs.fortinet.com/document/fortigate/6.4.0/new-features/228374/add-arrp-profile-for-wireless-controller-6-4-2

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**