Number: NSE6_FWF-6.4
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: NSE6_FWF-6.4

Exam Name: Fortinet NSE 6 - Secure Wireless LAN 6.4

Exam A

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

Correct Answer: B
Section:
Explanation:
FortiPlanner is a wireless network planning and deployment tool that helps to design and optimize wireless networks based on various parameters, such as floor plans, AP models, coverage areas, and client density.
FortiPlanner uses a predictive model in wireless design projects, which means that it estimates the wireless coverage and performance based on mathematical calculations and simulations, without requiring any physical measurements or site surveys.
Reference:FortiOS 6.4.0 Handbook - Wireless Controller, page 5; [FortiPlanner User Guide], page 9.

QUESTION 2
Refer to the exhibits.
Exhibit A

```
config wireless-controller wtp
    edit "FPXXXXXXXXXXXXXX"
        set admin enable
        set name "Authors AP1"
        set wtp-profile "Authors"
        config radio-1
        end
        config radio-2
        end
    next
    edit "FPXXXXXXXXXXXYYY"
        set admin enable
        set name " Authors AP2"
        set wtp-profile "Authors"
        config radio-1
        end
        config radio-2
        end
    next
    edit "FPXXXXXXXXXXXZZZ"
        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: A, C
Section:
Explanation:
The configuration changes that will resolve the issue are to configure set vaps to be ''Authors'' for both interfaces in the wtp-profile, and to configure vap-all to be manual for both interfaces in the wtp-profile. This is because the current configuration does not assign any VAPs to the AP interfaces, which means that no wireless networks are broadcasted by the APs. The vap-all setting determines whether all VAPs are assigned to an interface or not, and the vaps setting specifies which VAPs are assigned to an interface. By setting vap-all to manual and vaps to ''Authors'', the APs will only broadcast the Authors wireless network on both interfaces. Disabling intra-vap-privacy for the Authors vap-wireless network will not help, as it only affects the communication between clients on the same SSID, not their connection to the AP. Increasing the transmission power of the AP radio interfaces will not help, as it only affects the signal strength and coverage of the APs, not their broadcasting of wireless networks.
Reference:wireless-controller vap | FortiGate / FortiOS 6.4.0,Technical Note: How to configure intra-SSID privacy

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
Section:
Explanation:
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.

QUESTION 4
As standard best practice, which configuration should be performed before configuring FortiAPs using a FortiGate wireless controller?

A. Create wireless LAN specific policies
B. Preauthorize APs
C. Create a custom AP profile
D. Set the wireless controller country setting

Correct Answer: D
Section:
Explanation:
Setting the wireless controller country setting is a standard best practice that should be performed before configuring FortiAPs using a FortiGate wireless controller. The country setting determines the regulatory domain and the allowed channels and power levels for the wireless network. The country setting must match the physical location of the FortiAPs to comply with local regulations and avoid interference issues.
Reference:Secure Wireless LAN Course Description, page 5;FortiOS 6.4.0 Handbook - Wireless Controller, page 24.

QUESTION 5
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 county code settings on the profile
D. Create a new FortiAP profile and change the county code settings on the profile

Correct Answer: D
Section:
Explanation:
The correct way to ensure that the RF channels and transmission power limits are appropriately configured for the remote APs is to create a new FortiAP profile and change the country code settings on the profile. This is because the country code settings determine the legal RF channels and transmission power limits for each country, and they are applied at the FortiAP profile level. By creating a new FortiAP profile for the remote APs, you can specify the correct country code for Germany and assign it to the APs. This will ensure that the APs comply with the local regulations and avoid interference with other devices. Configuring the APs individually by overriding the settings in Managed FortiAPs is not recommended, as it is tedious and error-prone. Configuring the controller for the correct country code for Germany is not possible, as the controller can only have one country code setting, which should match its physical location. Cloning a suitable FortiAP profile and changing the county code settings on the profile is not advisable, as it may cause conflicts with other settings that are specific to the original profile.
Reference:Secure Wireless LAN course description, [FortiOS 6.4.0 Handbook - Wireless Controller]

QUESTION 6
Which two statements about background rogue scanning are correct? (Choose two.)

A. A dedicated radio configured for background scanning can support the connection of wireless clients
B. When detecting rogue APs, a dedicated radio configured for background scanning can suppress the rogue AP
C. Background rogue scanning requires DARRP to be enabled on the AP instance
D. A dedicated radio configured for background scanning can detect rogue devices on all other channels in its configured frequency band

Correct Answer: A, C
Section:

QUESTION 7
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

Correct Answer: A, B, E
Section:
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.
Dynamic VLAN allocation is a feature that allows wireless clients to be assigned to different VLANs based on RADIUS attributes returned by the authentication server. The three IETF attributes that must be supplied by the RADIUS server are: 81 Tunnel-Private-Group-ID, which specifies the VLAN ID for the client; 65 Tunnel-Medium-Type, which specifies the tunneling protocol as IEEE-802 (Ethernet); and 64 Tunnel-Type, which specifies the tunneling method as VLAN.
Reference:FortiOS 6.4.0 Handbook - Wireless Controller, page 60;FortiAP / FortiWiFi 6.4.0 Administration Guide, page 68.

QUESTION 8

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: A, C
Section:
Explanation:
According to the web search results, the project information phase and the site survey phase are part of the process to plan a wireless design project. The project information phase involves defining the project scope, objectives, requirements, deliverables, and stakeholders.It also includes creating a project plan, a risk management plan, a communication plan, and a budget.1The site survey phase involves conducting a physical inspection of the site where the wireless network will be deployed, measuring the signal strength and interference levels, identifying the optimal locations for the access points and antennas, and validating the network performance and coverage.2The hardware selection phase and the installation phase are not part of the planning process, but rather part of the implementation process.The hardware selection phase involves choosing the appropriate wireless devices, such as access points, routers, switches, controllers, and cables, based on the network design and specifications.3The installation phase involves installing, configuring, testing, and documenting the wireless network components according to the project plan and best practices.3Reference:Wireless Device Network Planning and Design - Emerson,Telecommunications and Implementation Project Management - BICSI,Project Planning | Wireless Design Services | Digi International

QUESTION 9
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: A, D
Section:
Explanation:
The control channel for managing traffic, which is always encrypted by DTLS. l The data channel for carrying client data packets.
When enabling security fabric on the FortiGate interface to manage FortiAPs, two types of communication channels are established between FortiGate and FortiAPs: control channels and data channels. Control channels are used for management and configuration of the FortiAPs, such as firmware updates, provisioning, and monitoring. Data channels are used for tunneling wireless traffic from the FortiAPs to the FortiGate for security inspection and policy enforcement.
Reference:FortiOS 6.4.0 Handbook - Security Fabric, page 17;FortiOS 6.4.0 Handbook - Wireless Controller, page 15.

QUESTION 10
Part of the location service registration process is to link FortiAPs in FortiPresence.
Which two management services can configure the discovered AP registration information from the FortiPresence cloud? (Choose two.)

A. AP Manager
B. FortiAP Cloud
C. FortiSwitch
D. FortiGate

Correct Answer: B, D
Section:
Explanation:
FortiGate, FortiCloud wireless access points (send visitor data in the form of station reports directly to FortiPresence)

Part of the location service registration process is to link FortiAPs in FortiPresence, which is a cloud-based service that provides location analytics and customer engagement tools for wireless networks. The management services that can configure the discovered AP registration information from the FortiPresence cloud are FortiAP Cloud and FortiGate. FortiAP Cloud is a cloud-based wireless LAN management platform that can discover, configure, monitor, and troubleshoot FortiAP devices. FortiGate is a network security appliance that can act as a wireless controller and manage FortiAP devices through security fabric or CAPWAP protocols.
Reference:FortiPresence Data Sheet, page 1;FortiOS 6.4.0 Handbook - Wireless Controller, page 9.

QUESTION 11
Which two configurations are compatible for Wireless Single Sign-On (WSSO)? (Choose two.)

A. A VAP configured for captive portal authentication
B. A VAP configured for WPA2 or 3 Enterprise
C. A VAP configured to authenticate locally on FortiGate
D. A VAP configured to authenticate using a radius server

Correct Answer: B, D
Section:
Explanation:
In the SSID choose WPA2-Enterprise authentication.
WSSO is RADIUS-based authentication that passes the user's user group memberships to the FortiGate.
Wireless Single Sign-On (WSSO) is a RADIUS-based authentication method that passes the user's user group memberships to the FortiGate for policy enforcement. WSSO can be configured for a VAP that uses WPA2 or WPA3 Enterprise authentication, which requires users to enter their credentials when connecting to the wireless network. WSSO can also be configured for a VAP that authenticates users using a RADIUS server, which returns the user group information in the Fortinet-Group-Name attribute.
Reference:FortiOS 6.4.0 Handbook - Wireless Controller, page 57;FortiOS 6.4.0 Handbook - Authentication, page 59.

QUESTION 12
Where in the controller interface can you find a wireless client's upstream and downstream link rates?

A. On the AP CLI, using the cw_diag ksta command
B. On the controller CLI, using the diag wireless-controller wlac -d sta command
C. On the AP CLI, using the cw_diag -d sta command
D. On the controller CLI, using the WiFi Client monitor

Correct Answer: A
Section:

QUESTION 13
Which administrative access method must be enabled on a FortiGate interface to allow APs to connect and function?

A. Security Fabric Connection
B. SSH
C. HTTPS
D. FortiTelemetry

Correct Answer: A
Section:

QUESTION 14
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.

Correct Answer: D
Section:
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.

QUESTION 15
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

Correct Answer: A, C
Section:
Explanation:
FortiPresence analytics is a cloud-based service that provides location analytics and customer engagement tools for wireless networks. FortiPresence analytics assists in generating presence reports by gathering details about on-site visitors, such as their dwell time, frequency, loyalty, and demographics. FortiPresence analytics also assists in comparing current data with historical records, such as trends, patterns, and anomalies.
Reference: [FortiPresence Data Sheet], page 1;FortiOS 6.4.0 Handbook - Wireless Controller, page 9.

QUESTION 16
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

Correct Answer: C
Section:
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 17
A tunnel mode SSID is configured on a FortiGate wireless controller.
Which task must be completed before the SSID can be used?

A. The new network must be manually assigned to a FortiAP profile.
B. The wireless network interface must be assigned a Layer 3 address.
C. Security Fabric and HTTPS must be enabled on the wireless network interface.

D. The wireless network to Internet firewall policy must be configured.

Correct Answer: B
Section:
Explanation:
The wireless network interface must be assigned a Layer 3 address because it acts as the gateway for the tunnel mode SSID traffic. The FortiGate wireless controller uses this interface to communicate with the FortiAPs and the wireless clients. Without a valid IP address, the tunnel mode SSID cannot function properly.
Reference:Secure Wireless LAN Course Description, page 5; [FortiOS 6.4.0 Handbook - Wireless Controller], page 24.

QUESTION 18
When using FortiPresence as a captive portal, which two types of public authentication services can be used to access guest Wi-Fi? (Choose two.)

A. Social networks authentication
B. Software security token authentication
C. Short message service authentication
D. Hardware security token authentication

Correct Answer: A, C
Section:
Explanation:
According to the web search results, FortiPresence supports social networks authentication and short message service authentication as public authentication services for guest Wi-Fi access. Social networks authentication allows visitors to log in using their existing social media accounts, such as Facebook, Twitter, LinkedIn, Google, and Instagram. Short message service authentication allows visitors to receive a one-time password via SMS to their mobile phone number. These authentication methods are convenient and secure for visitors and provide valuable data for businesses. Software security token authentication and hardware security token authentication are not supported by FortiPresence as public authentication services for guest Wi-Fi access.
Reference:Configuring Captive Portal | FortiPresence 1.2.0,Configuring Captive Portal | FortiPresence 22.4.0