www.atmicnetworks.com

ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

www.atmicnetworks.com

Question: 1

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:
According to Fortinet training: "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: 2

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: C

Explanation:

Question: 3

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: A, D

Explanation:

According to the web search results, Auto TX Power control is a feature that allows the AP to automatically adjust its transmission power based on the RF environment. The goal is to minimize interference and optimize coverage cells for roaming. When the AP detects any other wireless signal stronger than -70 dBm, it means that there is a potential source of interference nearby, so it will reduce its transmission power until it reaches the minimum configured TX power limit. This will reduce the interference and improve coexistence with other devices. When the AP detects any interference from a trusted neighboring AP stronger than -70 dBm, it means that there is a high density of APs in the area, so it will also reduce its transmission power until it reaches the minimum configured TX power limit. This will balance the load and avoid overlapping coverage areas. Reference: AP Transmit Power and Enable Power Reduction with Auto TX, Transmit Power and Antenna Configuration, Meraki Auto RF: Wi-Fi Channel and Power Management

Question: 4

Refer to the exhibits.

Exhibit A

```
config wireless-controller wtp-profile

    edit "Main Networks - FAP-320C"
        set comment "Profile with standard networks" config platform
            set type 320C
        end
        set handoff rssi 30
        set handoff-sta-thresh 30
        set ap-country GB

        config radio-1
            set band 802.lln

            set power-level 50
            set channel-utilization enable
            set wids-profile "default-wids-apscan-enabled" set darrp enable

            set vap-all manual
            set vaps "Main-Wifi" "Contractors" "Guest" "WifilOT" "WifiPOS" "Staff"
```

www.atmicnetworks.com

```
"Students"
            set channel "1" "6" "11" end

        config radio-2
            set band 802.11ac

            set channel-bonding 40MHz
            set power-level 60
            set channel-utilization enable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable

            set vap-all manual
            set vaps "Main-Wifi" "Contractors" "Guest" "WifilOT" "WifiPOS" "Staff"
"Students"

            set channel "36" "44" "52" "60"
        end next end
```

Exhibit B

www.atmicnetworks.com

Diagnostics and Tools • Office

*i Office

Serial Number	FPXXXXXXXXXXX
Base MAC Address	xx:xx:xx:xx:xx:xx
Status	© Online
Country/Reglon	GB
Uplink Interface	FortiAP management (ap)
IPv4 Address	192.168.5.98
Uptime	12m1s
Version	v6.4 build0437

Actions *

O General

■AS CPUUwce
■Z3B Memory UHft
■Ed Connection Uptime Uni

Q Radio 1-2.4 GHz

51 | Interfering SSIDs
1 | Clients
25% | Channel Utilization

3 Radio 2- 5 GHz

0 | Interfering SSIDs
30 | Clients
5% | Channel Utilization

Radios | Clients | Interfering SSIDs | Logs | CLI Access | Spectrum Analysis | VLAN Probe

	Radiol-2.4 GHz	Radio2-5GHz
Mode	AP	AP
SSID	►5 fortinet (Main-WiFi) H fortinet2 (Contractors) g fortinet3 (Guest)	« fortinet (Main-WiFi) fortinet2 (Contractors) " fortinet3 (Guest)
Clients	1	20
Bandwidth Tx	4.65 kbps	1.16 kbps
Bandwidth Rx	20.46 kbps	176 bps
Operating Channel Channels	1	60
Operating TX Power	3 dBm	21 dBm
Band	802.1 In	802.1 lac

Interfering SSIDs for Office (Radio 1) x

0 Refresh Search Q

SSID *	AP BSSID*	Channel ▼	Signals
Husky	aa:aa:aa:aa:aa	1	.□ -84 dBm
Husky guest	bb:bb:bb:bb:bb	1	-84 dBm
KBANK5007	ccxcxcxcxcxc	1	-85 dBm
mandikaylee	dd:dd:dd:dd:dd	1	-86 dBm
	ee:ee:ee:ee:ee	1	-87 dBm
HUAWEI-EMIX4f	ee:ee:ee:ee:ef	1	jf I -88 dBm
trojan-3	ff:ff:ff:ff;ff:ff	1	-88 dBm
	fg:gg:gg:gg:gg	1	jf -89 dBm
	hg:gg:gg:gg:gg	1	-89 dBm

Exhibit C

```
1 get wireless-controller rf-analysis FPXXXXXXXXXXXXX

WTP: Office 0-192.168.5.98:5246
```

channel	rssi-total	rf-score	overlap-ap	interfere-ap	chan-utilization
1	100	6	13	13	63%
2	23	10	0	22	47%
3	15	10	0	22	15%
4	24	10	0	22	15%
5	51	10	0	22	41%
6	223	1	9	9	75%
7	52	10	0	17	47%
8	32	10	0	17	13%
9	27	10	0	19	10%
10	45	10	D	19	28%
11	177	1	8	10	65%
12	46	10	0	10	34%
13	45	10	2	10	70%
14	14	10	0	10	0%
36	16	10	2	2	0%
44	83	7	5	5	0%

A wireless network has been installed in a small office building and is being used by a business to connect its wireless clients. The network is used for multiple purposes, including corporate access, guest access, and connecting point-of-sale and IoT devices.

Users connecting to the guest network located in the reception area are reporting slow performance. The network administrator is reviewing the information shown in the exhibits as part of the ongoing investigation of the problem. They show the profile used for the AP and the controller RF analysis output together with a screenshot of the GUI showing a summary of the AP and its neighboring APs. To improve performance for the users connecting to the guest network in this area, which configuration change is most likely to improve performance?

A. Increase the transmission power of the AP radios
B. Enable frequency handoff on the AP to band steer clients
C. Reduce the number of wireless networks being broadcast by the AP
D. Install another AP in the reception area to improve available bandwidth

Answer: B

Explanation:

Question: 5

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

Answer: AC

Explanation:

Question: 6

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: A, B, E

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
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: 7

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

Answer: AC

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.1 The 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.2 The 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.3 The installation phase involves installing, configuring, testing, and documenting the wireless network components according to the project plan and best practices.3 Reference: Wireless Device Network Planning and Design - Emerson, Telecommunications and Implementation Project Management - BICSI, Project Planning | Wireless Design Services | Digi International

Question: 8

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

Answer: A, D

Explanation:

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- ce67-11e9-8977-00505692583a/FortiWiFi_and_FortiAP-6.2-Cookbook.pdf
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: 9

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

Answer: B, D

Explanation:

FortiGate, FortiCloud wireless access points (send visitor data in the form of station reports directly to FortiPresence)
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/df877622- c976-11e9-8977-00505692583a/FortiPresence-v4.3-release-notes.pdf
Part of the location service registration process is to link FortiAPs in FortiPresence, which is a cloudbased 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: 10

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

Answer: B, D

Explanation:

In the SSID choose WPA2-Enterprise authentication.
WSSO is RADIUS-based authentication that passes the user's user group memberships to the FortiGate.
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/b92a67f9- 73a6-11ea-9384-00505692583a/FortiWiFi_and_FortiAP-6.4.2-Configuration_Guide.pdf
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: 11

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

Answer: A

Explanation:

Question: 12

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

Answer: A

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

Question: 13

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

Question: 14

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: A, C

Explanation:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/457ebad4- 2437-11e9-b20a-f8bc1258b856/FortiPresence-v2.0-getting-started.pdf
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: 15

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 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: 16

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

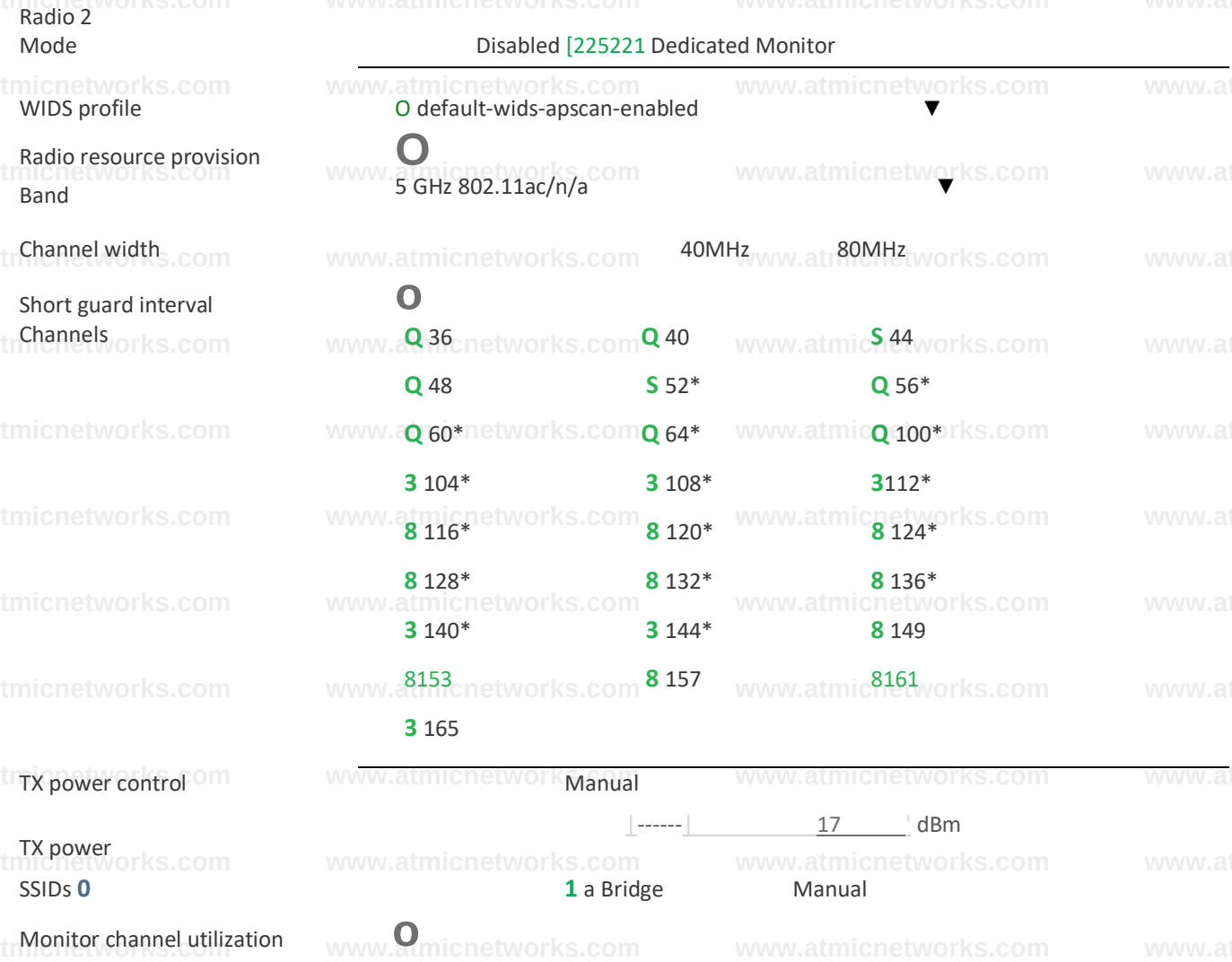
A. Create wireless LAN specific policies
B. Preauthorize APs
C. Create a custom AP profile
D. Set the wireless controller country setting

Answer: D

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: 17

Refer to the exhibit.



What does the asterisk (*) symbol beside the channel mean?

A. Indicates channels that can be used only when Radio Resource Provisioning is enabled
B. Indicates channels that cannot be used because of regulatory channel restrictions
C. Indicates channels that will be scanned by the Wireless Intrusion Detection System (WIDS)
D. Indicates channels that are subject to dynamic frequency selection (DFS) regulations

Answer: D

Explanation:
This frequencies are also used by other licensed applications, wireless LANs have to use a specific method to gain access to certain higher frequencies and this method is known as DFS.

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

Answer: A, C

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

Question: 19

Six APs are located in a remotely based branch office and are managed by a centrally hosted FortiGate. Multiple wireless users frequently connect and roam between the APs in the remote office.
The network they connect to, is secured with WPA2-PSK. As currently configured, the WAN connection between the branch office and the centrally hosted FortiGate is unreliable.
Which configuration would enable the most reliable wireless connectivity for the remote clients?

A. Configure a tunnel mode wireless network and enable split tunneling to the local network
B. Configure a bridge mode wireless network and enable the Local standalone configuration option
C. Configure a bridge mode wireless network and enable the Local authentication configuration option
D. Install supported FortiAP and configure a bridge mode wireless network

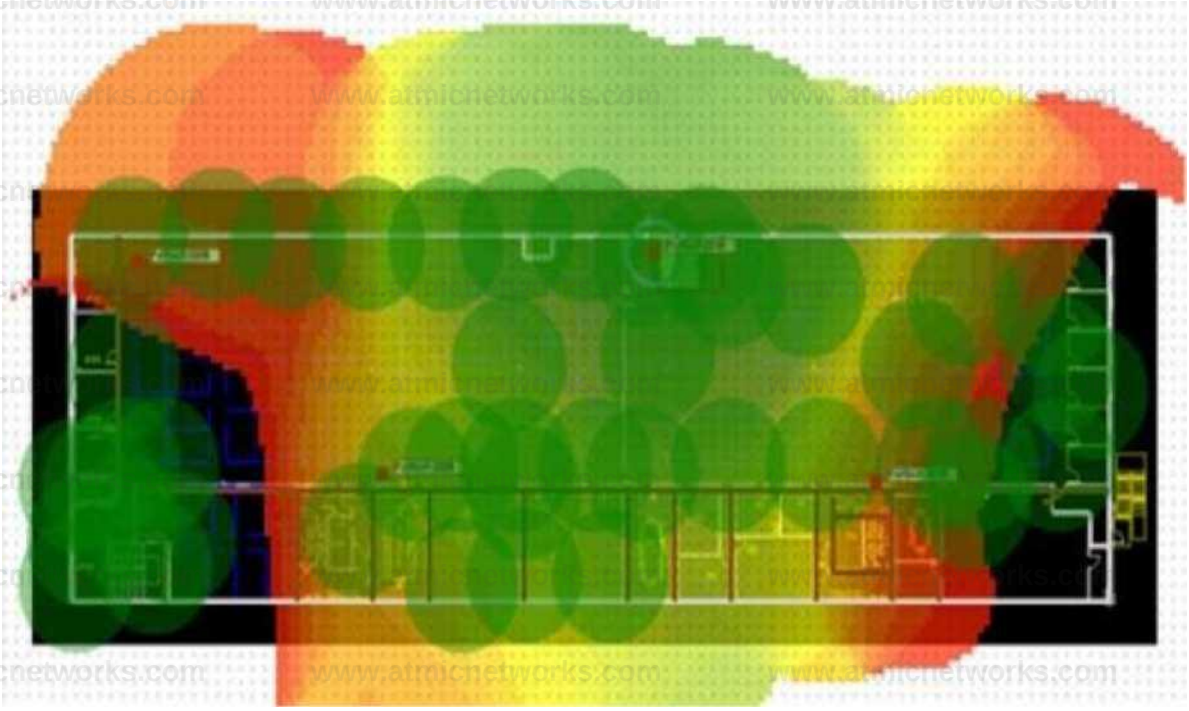
Answer: B

Explanation:

Look for “Continued FortiAP operation when WiFi controller connection is down” im the link here:
https://docs.fortinet.com/document/fortiap/7.0.4/fortiwifi-and-fortiap-configuration- guide/442078/how-to-configure-a-fortiap-local-bridge-private-cloud-managed-ap

Question: 20

Refer to the exhibit.



If the signal is set to -68 dB on the FortiPlanner site survey reading, which statement is correct regarding the coverage area?

A. Areas with the signal strength equal to -68 dB are zoomed in to provide better visibility
B. Areas with the signal strength weaker than -68 dB are cut out of the map
C. Areas with the signal strength equal or stronger than -68 dB are highlighted in multicolor
D. Areas with the signal strength weaker than -68 dB are highlighted in orange and red to indicate that no signal was propagated by the APs.

Answer: C

Explanation:

Question: 21

Which statement describes FortiPresence location map functionality?

A. Provides real-time insight into user movements
B. Provides real-time insight into user online activity
C. Provides real-time insight into user purchase activity
D. Provides real-time insight into user usage stats

Answer: A

Explanation:
(Page 88 Study Guide) "FortiPresence provides data and analytics based on demographic segmentation and visitor movement between areas"

According to the web search results, FortiPresence location map functionality provides real-time

www.atmicnetworks.com

insight into user movements. It uses the location data from the Fortinet access points to detect each visitor's smartphone Wi-Fi signal and track their location and behavior within the site. It also provides data visualization in a customizable format, such as heat maps and animated flows, to show the visitor traffic and movement patterns. This geographical data analysis can help improve visitor experiences and business outcomes. Reference: Location Analytics | FortiPresence 22.4.0 - Fortinet Documentation, FortiPresence Data Sheet

Question: 22

Refer to the exhibits.

Exhibit A

53836.574 xx:xx:xx:xx:xx:xx <ih> IEEE 802.11 mgmt::assoc req <== xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rid 1 wld2 yy;yy:yy:yy:yy:yy

53836.574 xx:xx:xx:xx:xx:xx <ih> xx:xx:xx:xx:xx:xx sta = 0x6311c88, sta->flags = 0x00000001, authalg = 0, hapd->splitMac: 1

53836.575 xx:xx:xx:xx:xx:xx <ih> IEEE 802.11 mgmt::assoc resp <= xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rid 1 wld2 yy:yy:yy:yy:yy=yy

53836.575 xx:xx:xx:xx:xx:xx <ih> IEEE 802.11 mgmt::assocresp <== xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) vap Wireless rid 1 wld2 yy=yy:yy:yy:yy:yy

53836.575 xx:xx:xx:xx:xx:xx <dc> STA add xx:xx:xx:xx:xx:xx vap Wireless ws (0-192.168.5.98:5246) rid 1 wld2 bssid yy:yy:yy:yy:yy:yy NON-AUTH band oxio mimo 2*2

53836.575 xx:xx:xx:xx:xx:xx <cc> STA CFG REQ(10) sta xx:xx:xx:xx:xx:xx add ==> ws (0-192.168.5.98:5246) rid 1 wld 2

53836.576 xx:xx:xx:xx:xx:xx <cc> STA add xx:xx:xx:xx:xx:xx vap Wireless ws (0-192.168.5.98:5246) rid 1 wld 2 yy:yy:yy:yy:yy:yy sec WPA2 PERSONAL auth 0

53836.576 xx:xx:xx:xx:xx:xx cwAcStaRbtAdd: I2C STA ADD insert sta xx:xx:xx:xx:xx:xx 192.168.5.98/1/2/1

53836.577 xx:xx:xx:xx:xx:xx <cc> STA CFGRESP(IO) sta xx:xx:xx:xx:xx:xx <== ws (0-192.168.5.98:5246) rc 0 (Success)

64318.579 xx:xx:xx:xx:xx:xx <eh> RADIUS message (type=0) ==> RADIUS Server code=l (Access-Request) id=9 len=214

64318.579 xx:xx:xx:xx:xx:xx <eh> send 1/4 msg of 4-Way Handshake

64318.580 xx:xx:xx:xx:xx:xx <eh> send IEEE 802.IX ver=2 type=3 (EAPOL KEY) data len=95 replay ent 1

64813.580 xx:xx:xx:xx:xx:xx <eh> IEEE 802.IX (EAPOL99B) ==> xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rid 1 wld 2 yy=yy:yy:yy:yy:yy

64318.582 xx:xx:xx:xx:xx:xx <eh> RADIUS message (type=0) <= RADIUS Server code=2 (Access-Accept) id=9 len=114

53836.582 xx:xx:xx:xx:xx:xx <dc> STA chg xx:xx:xx:xx:xx:xx vap Wireless ws (0-192.168.5.98:5246) rid 1 wld 2 bssid yy:yy:yy:yy:yy:yy Auth:ailow

Exhibit B

64813.583 xx:xx:xx:xx:xx:xx <eh> IEEE 802.IX (EAPOL 121B) <== xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rid 1 wld2 yy:yy:yy:yy:yy=yy

64813.583 xx:xx:xx:xx:xx:xx <eh> recv IEEE 802.IX ver=l type=3 (EAPOL KEY) data len=117

64813.583 xx:xx:xx:xx:xx:xx <eh> recv EAPOL-Key 2/4 Pairwise replay ent 1

64813.583 xx:xx:xx:xx:xx:xx <eh> send 3/4 msg of 4-Way Handshake

64813.584 xx:xx:xx:xx:xx:xx <eh> send IEEE 802.IX ver=2 type=3 (EAPOLKEY) data len=151 replay ent 2

```
64813.584 xx:xx:xx:xx:xx:xx <eh> IEEE 802.IX (EAPOL 155B) => xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rid 1 wld2 yy:yy:yy:yy;yy:yy

64813.586 xx:xx:xx:xx:xx:xx <eh> IEEE 802.IX (EAPOL 99B) <= xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rid 1 wld2 yy:yy:yy:yy=yy:yy

64813.586 xx:xx:xx:xx:xx:xx <eh> recv IEEE 802.IX ver=l type=3 (EAPOL KEY) data len=35

64813.586 xx:xx:xx:xx:xx:xx <eh> recv EAPOL-Key 4/4 Pairwise replay ent 2

53836.587 xx:xx:xx:xx:xx:xx <dc> STA chg xx:xx:xx:xx:xx:xx vap Wireless ws (0-192.168.5.98:5246) rid 1 wld2 bssid yy:yy:yy:yy=yy:yy AUTH

53836.587 xx:xx:xx:xx:xx:xx <cc> STA chg xx:xx:xx:xx:xx:xx vap Wireless ws (0-192.168.5.98:5246) rid 1 wld2 yy:yy:yy:yy:yy:yy sec WPA2 PERSONAL auth 1 ******

53836.587 xx:xx:xx:xx:xx:xx <cc> STA_CFG_REQ(12) sta xx:xx:xx:xx:xx:xx add key (len=16) ==> ws (0-192.168.5.98:5246) rid 1 wld2

53836.589 xx:xx:xx:xx:xx:xx <cc> STA_CFG_REQ(12) xx:xx:xx:xx:xx:xx <== ws (0-192.168.5.98:5246) re 0 (Success)

53837.140 xx:xx:xx:xx:xx:xx <dc> DHCP Request server 0.0.0.0 <== host DESKTOP-CVKGHH mac xx:xx:xx:xx:xx:xx ip 192.168.30.2 xld 88548005

53837.142 xx:xx:xx:xx:xx:xx <dc> DHCP Ack server 192.168.30.1 —> host mac xx:xx:xx:xx:xx:xx ip 192.168.30.2 mask 255.255.255.0 gw 192.168.30.1 xld 88548005
```

The exhibits show the diagnose debug log of a station connection taken on the controller CLI. Which security mode is used by the wireless connection?

A. WPA2 Enterprise
B. WPA3 Enterprise
C. WPA2 Personal and radius MAC filtering
D. Open, with radius MAC filtering

Answer: C

Explanation:

Question: 23

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

Answer: A

Explanation:
https://docs.fortinet.com/document/fortipresence-vm/1.2.0/administration- guide/546812/introduction

Question: 24

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

Answer: D

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: 25

Refer to the exhibits.
Exhibit A

```
config wireless-controller wtp edit "FPXXXXXXXXXXXXX" set
admin enable set name "Authors API" set wtp-profile "Authors"
config radio-1 end config radio-2 end next edit
"FPXXXXXXXXXXYYY" 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.lln, 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

Answer: A, C

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: 26

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: C

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.

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/723e20ad-5098-11e9-94bf-00505692583a/FortiWiFi_and_FortiAP-6.2.0-Configuration_Guide.pdf

Question: 27

What is the first discovery method used by FortiAP to locate the FortiGate wireless controller in the default configuration?

A. DHCP

B. Static
C. Broadcast
D. Multicast

Answer: B

Explanation:
According to the web search results, the first discovery method used by FortiAP to locate the FortiGate wireless controller in the default configuration is static. This means that the FortiAP sends discovery requests to a preconfigured IP address that the controller owns. This is useful if the FortiAP and the controller are not in the same subnet and other discovery methods will not work. The other discovery methods are used in sequence if the static method fails or is not configured.
Reference: Advanced WiFi controller discovery | FortiAP / FortiWiFi 7.4.0

Question: 28

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

Answer: BD

Explanation:

Question: 29

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:
Reference: https://docs.fortinet.com/document/fortiap/6.4.0/fortiwifi-and-fortiap-configuration- guide/47321/fortiap-s-bridge-mode-security-profiles
If a bridge mode SSID is configured for a managed FortiAP, you can add a security profile group to the wireless controller, if the FortiAP model supports the security profile. This is supported only in bridge mode.

Question: 30

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.

Reference: https://docs.fortinet.com/document/fortiap/7.0.1/fortiwifi-and-fortiap-configuration-guide/376326/configuring-dynamic-user-vlan-assignment

Question: 31

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.

Answer: B

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: 32

How can you find upstream and downstream link rates of a wireless client using FortiGate?

A. On the FortiAP CLI, using the cw_diag ksta command

B. On the FortiAP CLI, using the cw_diag -d sta command

C. On the FortiGate GUI, using the WiFi Client monitor

D. On the FortiGate CLI, using the diag wireless-controller wlac -d Sta command

Answer: C

Explanation:

The WiFi Client monitor on the FortiGate GUI shows the upstream and downstream link rates of a wireless client, along with other information such as MAC address, SSID, IP address, signal strength, and connection time. The link rates indicate the maximum data rates that the client can achieve in both directions. Reference: Secure Wireless LAN Course Description, page 7; [FortiOS 6.4.0 Handbook - Wireless Controller], page 37.

Question: 33

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.

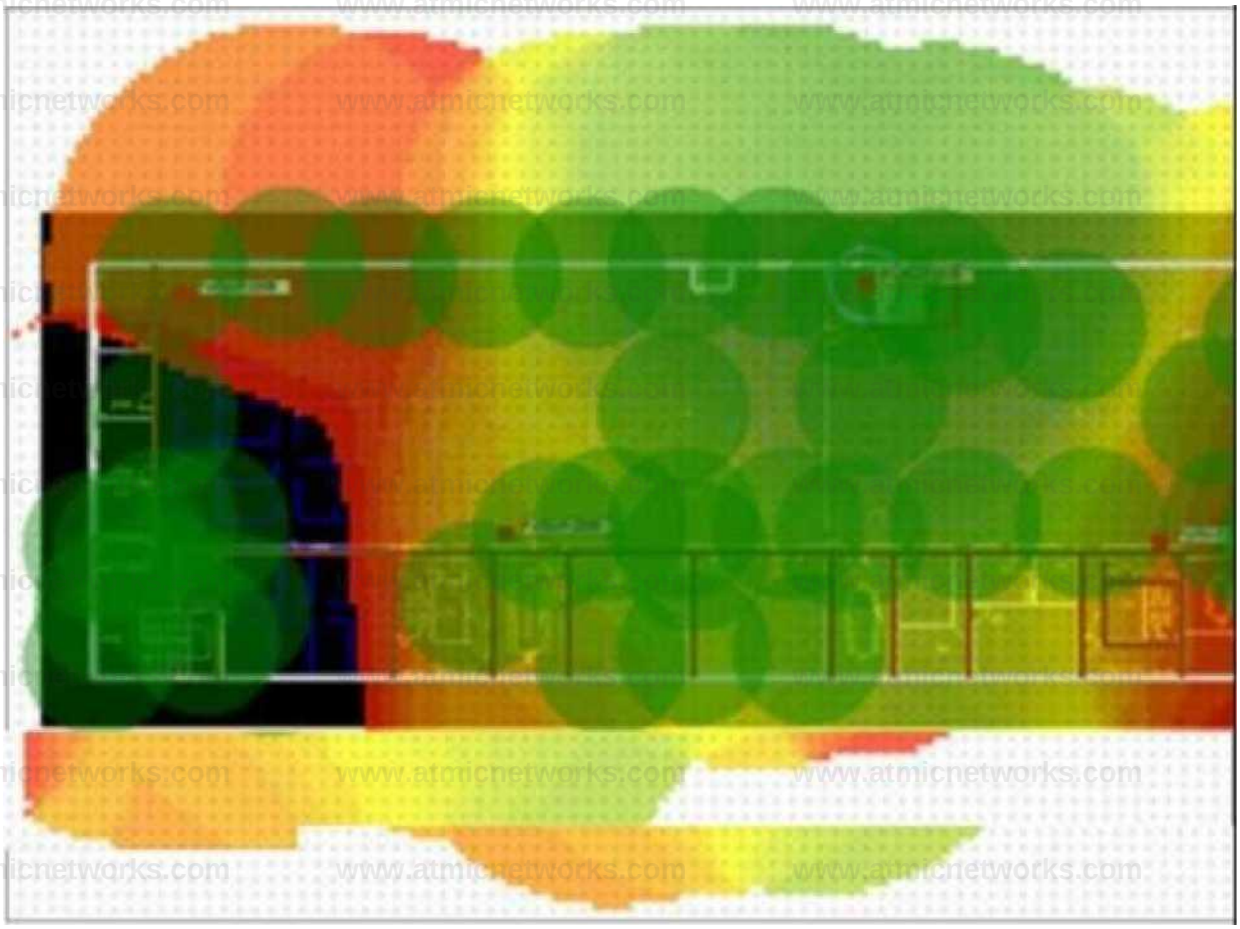
Answer: D

Explanation:

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. Reference: Secure Wireless LAN Course Description, page 9; [FortiOS 6.4.0 Handbook - Wireless Controller], page 46.

Question: 34

Refer to the exhibit.



If the signal is set to -68 dB on the FortiPlanner site survey reading, which statement is correct regarding the coverage area?

A. Areas with the signal strength weaker than -68 dB are shown with black background.

B. Areas with the signal strength equal to -68 dB are zoomed in to provide better visibility.

C. Areas with the signal strength weaker than -68 dB are highlighted in orange and red to indicate that no signal was propagated by the APS.

D. Areas with the signal strength equal or stronger than -68 dB are highlighted in green circles.

Answer: D

Explanation:

The FortiPlanner site survey reading is a tool that shows the predicted signal strength of the wireless network based on the floor plan, the placement of the APs, and the propagation model. The signal strength is measured in decibels (dB), which is a logarithmic scale that indicates how much power the signal has. The higher the dB value, the stronger the signal.

The site survey reading allows the user to set a threshold value for the signal strength, which is -68 dB by default. This means that any area with a signal strength equal or stronger than -68 dB is considered to have adequate coverage for most wireless applications. These areas are highlighted in green circles on the floor plan. Any area with a signal strength

weaker than -68 dB is considered to have poor coverage or no coverage at all. These areas are shown with different colors, such as yellow, orange, red, or black, depending on how weak the signal is.

Therefore, the correct answer is D. Areas with the signal strength equal or stronger than -68 dB are highlighted in green circles.

Reference:

FortiPlanner 2.0 User Guide, page 28

FortiPlanner Data Sheet, page 2

FortiPlanner 2.2 User Guide, page 19

Question: 35

Which statement is correct about security profiles on FortiAP devices?

A. Security profiles are only supported on Bridge-mode SSIDs.

B. Security profiles can only be applied via firewall policies on the FortiGate.

C. Security profiles can only be applied to unencrypted wireless traffic.

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

Answer: D

Explanation:

Security profiles are a feature that allows FortiAP devices to apply various security functions to the wireless traffic, such as antivirus, web filter, application control, intrusion prevention, and botnet scanning. Security profiles can be enabled on both tunnel-mode and bridge-mode SSIDs, and can be applied either through the wireless controller configuration or through firewall policies on the FortiGate device. Security profiles can also inspect encrypted wireless traffic, as long as the FortiAP device has access to the encryption keys.

Security profiles on FortiAP devices can use FortiGate subscription services to inspect the traffic, such as FortiGuard Antivirus, FortiGuard Web Filter, FortiGuard Application Control, and FortiGuard IPS. This means that the FortiAP device can leverage the latest threat intelligence and updates from Fortinet to protect the wireless network from malicious or unwanted content.

Therefore, the correct answer is D. Security profiles on FortiAP devices can use FortiGate subscription to inspect the traffic.

Reference:

FortiAP-S and FortiAP-U bridge mode security profiles

Configuring security | FortiAP / FortiWiFi 6.4.2

Security profiles - Fortinet Document Library