Fortinet.Pre. NSE6_FWF-6.4.by.VCEplus.30q - DEMO

Exam A

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.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/wireless/ap_wireless_signalstrength_c.html

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 802.11n
            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"
"Wifi_IOT" "Wifi_POS" "Staff" "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"
"Wifi_IOT" "Wifi_POS" "Staff" "Students"
            set channel "36" "44" "52" "60"
        end
    next
end
```

Exhibit B.

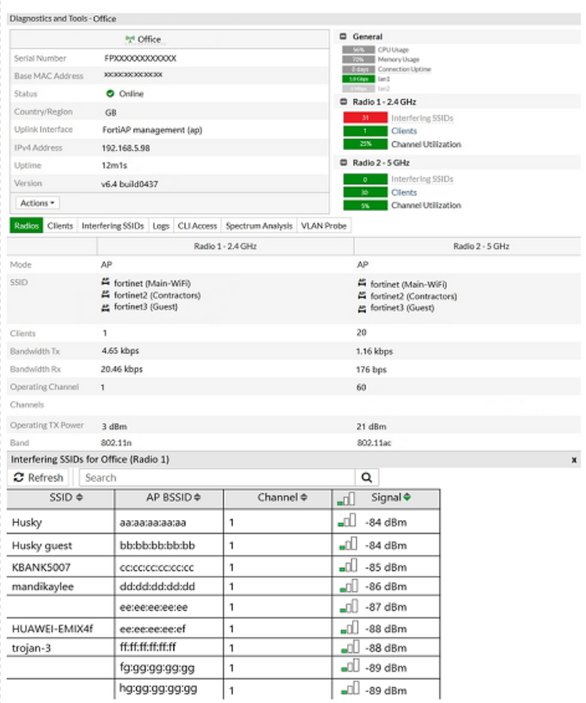


Exhibit C.

```
# 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           0              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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To enable rogue AP scanning

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 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

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
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 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

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.sciencedirect.com/topics/computer-science/wireless-site-survey
https://www.automation.com/en-us/articles/2015-2/wireless-device-network-planning-and-design

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The control channel for managing traffic, which is always encrypted by DTLS. I 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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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

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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: AB
Section: (none)
Explanation

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
FortiPlanner will look familiar to anyone who has used architectural or home design software.

Reference: http://en.hackdig.com/?7883.htm

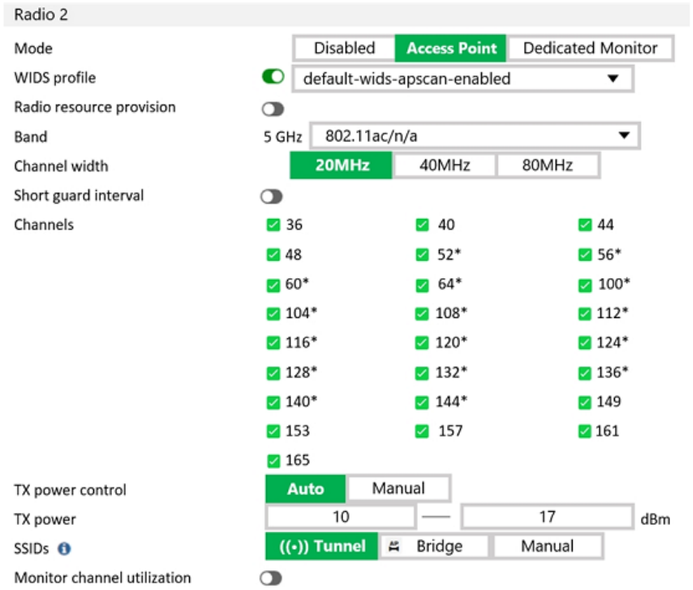
QUESTION 16
As standard best practice, which configuration should be performed before configuring FortiAPs using a FortiGate wireless controller?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.fortinet.com/document/fortiap/6.4.1/fortiwifi-and-fortiap-configuration-guide/547298/complex-wireless-network-example

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This information along with the social network authentication logins with Facebook, Google, Instagram, LinkedIn, or FortiPresence using your WiFi.

Captive Portal configurations for social media logins and internet access. You can add and manage sites using the integrated Google maps and manoeuvre your hardware infrastructure easily.

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/e126e498-eabb-11eb-97f7-00505692583a/FortiPresence-21.3-Administration_Guide.pdf

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.

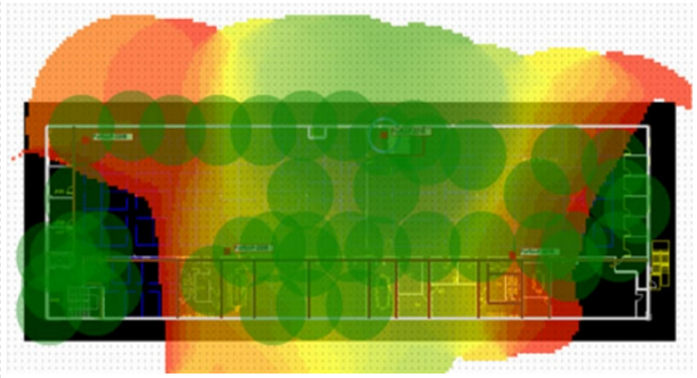
Which configuration would enable the most reliable wireless connectivity for the remote clients?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

This geographical data analysis provides real-time insights into user behavior.

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/05d8bae1-5f3c-11e9-81a4-00505692583a/FortiPresence-v2.0.1-getting-started.pdf

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 wId2
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, auth_alg = 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 wId2
yy:yy:yy:yy:yy:yy

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 wId2
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 wId2 bssid
yy:yy:yy:yy:yy:yy NON-AUTH   band 0x10 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 wId 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 wId 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_CFG_RESP(10) 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=1 (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 802.1X ver=2 type=3
(EAPOL_KEY) data len=95 replay cnt 1

64813.580 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL99B) ==>
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId 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 wId 2 bssid
yy:yy:yy:yy:yy:yy Auth:allow
```

Exhibit B

```
64813.583 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 121B) <--
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.583 xx:xx:xx:xx:xx:xx <eh>     recv IEEE 802.1X ver=1 type=3
(EAPOL_KEY) data len=117

64813.583 xx:xx:xx:xx:xx:xx <eh>     recv EAPOL-Key 2/4 Pairwise
replay cnt 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 802.1X ver=2 type=3
(EAPOL_KEY) data len=151 replay cnt 2

64813.584 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 155B) ==>
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.586 xx:xx:xx:xx:xx:xx <eh> IEEE 802.1X (EAPOL 99B) <==
xx:xx:xx:xx:xx:xx ws (0-192.168.5.98:5246) rId 1 wId2
yy:yy:yy:yy:yy:yy

64813.586 xx:xx:xx:xx:xx:xx <eh>     recv IEEE 802.1X ver=1 type=3
(EAPOL_KEY) data len=35

64813.586 xx:xx:xx:xx:xx:xx <eh>     recv EAPOL-Key 4/4 Pairwise
replay cnt 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 wId2 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 wId2 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 wId2

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) rc 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 xId
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 xId 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Best security option is WPA2-AES.

Reference: https://www.esecurityplanet.com/trends/the-best-security-for-wireless-networks/

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/69a8fa9c-1eaa-11e9-b6f6-f8bc1258b856/fortigate-fortiwifi-and-fortiap-configuration-guide-54.pdf

QUESTION 25
Refer to the exhibits.

Exhibit A

```
config wireless-controller wtp
    edit "FPXXXXXXXXXXXXX"
        set admin enable
        set name "Authors AP1"
        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 "FPXXXXXXXXXXZZZ"
        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: BC
Section: (none)
Explanation

Explanation/Reference:

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 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

Correct Answer: B
Section: (none)
Explanation

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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