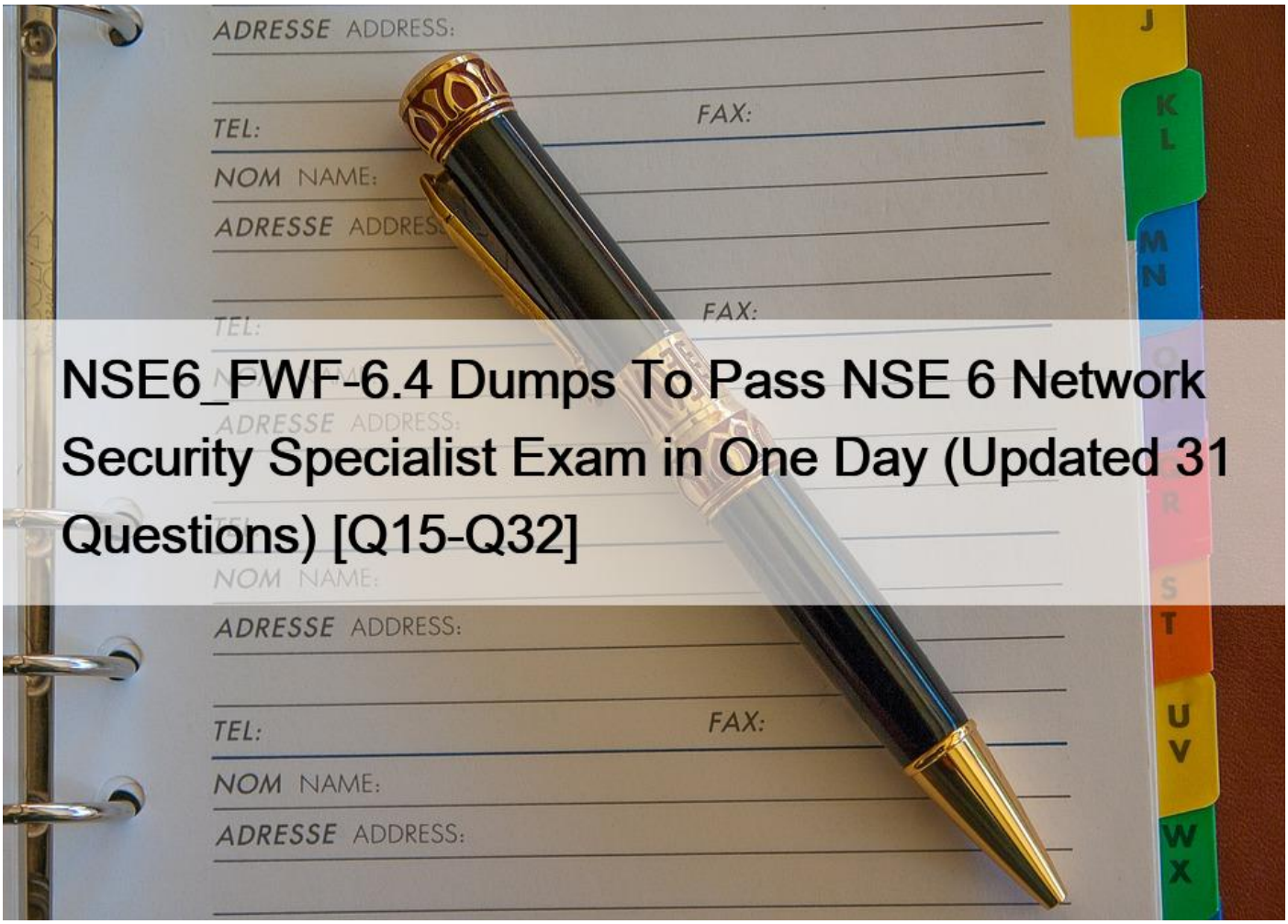
NSE6_FWF-6.4 Dumps To Pass NSE 6 Network Security Specialist Exam in One Day (Updated 31 Questions) [Q15-Q32



NSE6_FWF-6.4 Dumps To Pass NSE 6 Network Security Specialist Exam in One Day (Updated 31 Questions)
NSE6_FWF-6.4 Exam Brain Dumps - Study Notes and Theory

NO.15 Which two roles does FortiPresence analytics assist in generating presence reports? (Choose two.)
* Gathering details about on site visitors
* Predicting the number of guest users visiting on-site
* Comparing current data with historical records
* Reporting potential threats by guests on site

NO.16 Refer to the exhibits.

Exhibit A

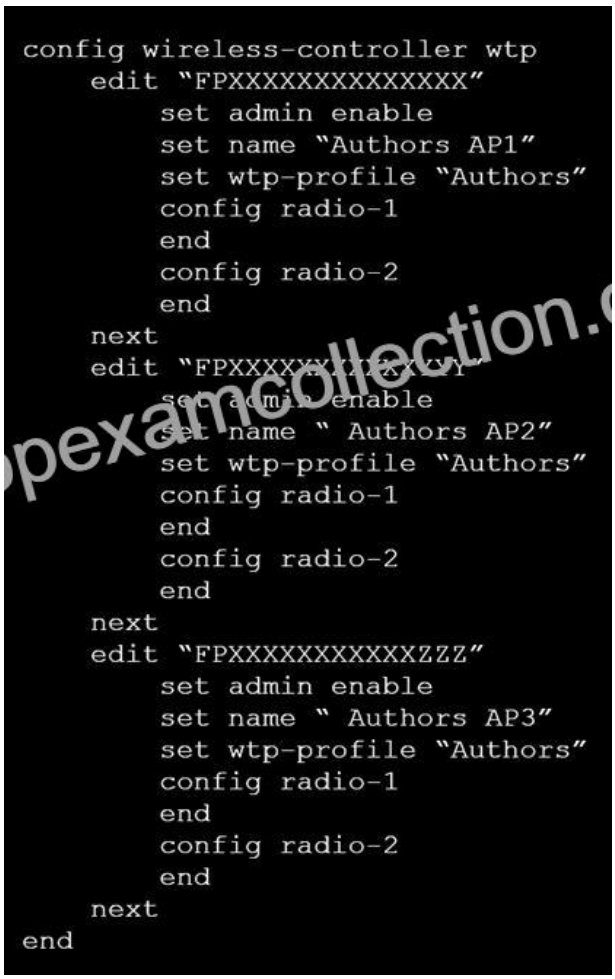

config wireless-controller wtp
edit "FPXXXXXXXXXXXXX"
set admin enable
set name "Authors AP1"
set wtp-profile "Authors"
config radio-1
end
config radio-2
end
next
edit "FPXXXXXXXXXXXXY"
set admin enable
set name " Authors AP2"
set wtp-profile "Authors"
config radio-1
end
config radio-2
end
next
edit "FPXXXXXXXXXXXZZZ"
set admin enable
set name " Authors AP3"
set wtp-profile "Authors"
config radio-1
end
config radio-2
end
next
end

Exhibit B

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.)

* For both interfaces in the wtp-profile, configure set vaps to be “Authors”
* Disable intra-vap-privacy for the Authors vap-wireless network
* For both interfaces in the wtp-profile, configure vap-all to be manual
* Increase the transmission power of the AP radio interfaces

NO.17 What is the first discovery method used by FortiAP to locate the FortiGate wireless controller in the default configuration?

* DHCP
* Static
* Broadcast
* Multicast

NO.18 Which statement describes FortiPresence location map functionality?
* Provides real-time insight into user movements
* Provides real-time insight into user online activity
* Provides real-time insight into user purchase activity
* Provides real-time insight into user usage stats

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

NO.19 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?
* Areas with the signal strength equal to -68 dB are zoomed in to provide better visibility
* Areas with the signal strength weaker than -68 dB are cut out of the map
* Areas with the signal strength equal or stronger than -68 dB are highlighted in multicolor
* 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.

NO.20 Which two phases are part of the process to plan a wireless design project? (Choose two.)
* Project information phase
* Hardware selection phase
* Site survey phase
* Installation phase

Reference:

https://www.automation.com/en-us/articles/2015-2/wireless-device-network-planning-and-design

NO.21 Which of the following is a requirement to generate analytic reports using on-site FortiPresence deployment?
* SQL services must be running
* Two wireless APs must be sending data
* DTLS encryption on wireless traffic must be turned off
* Wireless network security must be set to open

NO.22 As standard best practice, which configuration should be performed before configuring FortiAPs using a FortiGate wireless controller?
* Create wireless LAN specific policies
* Preauthorize APs
* Create a custom AP profile
* Set the wireless controller country setting

NO.23 What type of design model does FortiPlanner use in wireless design project?
* Architectural model
* Predictive model
* Analytical model
* Integration model

NO.24 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?

* WPA2 Enterprise
* WPA3 Enterprise

* WPA2 Personal and radius MAC filtering
* Open, with radius MAC filtering

Best security option is WPA2-AES.

NO.25 When using FortiPresence as a captive portal, which two types of public authentication services can be used to access guest Wi-Fi? (Choose two.)

* Social networks authentication
* Software security token authentication
* Short message service authentication
* Hardware security token authentication

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.

NO.26 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 "FPXXXXXXXXXXXXYY"
        set admin enable
        set name " Authors AP2"
        set wtp-profile "Authors"
        config radio-1
        end
        config radio-2
        end
    next
    edit "FPXXXXXXXXXXXXZZZ"
        set admin enable
        set name " Authors AP3"
        set wtp-profile "Authors"
        config radio-1
        end
        config radio-2
        end
    next
end
```

Exhibit B

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.)
* For both interfaces in the wtp-profile, configure set vaps to be “Authors”
* Disable intra-vap-privacy for the Authors vap-wireless network
* For both interfaces in the wtp-profile, configure vap-all to be manual
* Increase the transmission power of the AP radio interfaces

NO.27 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

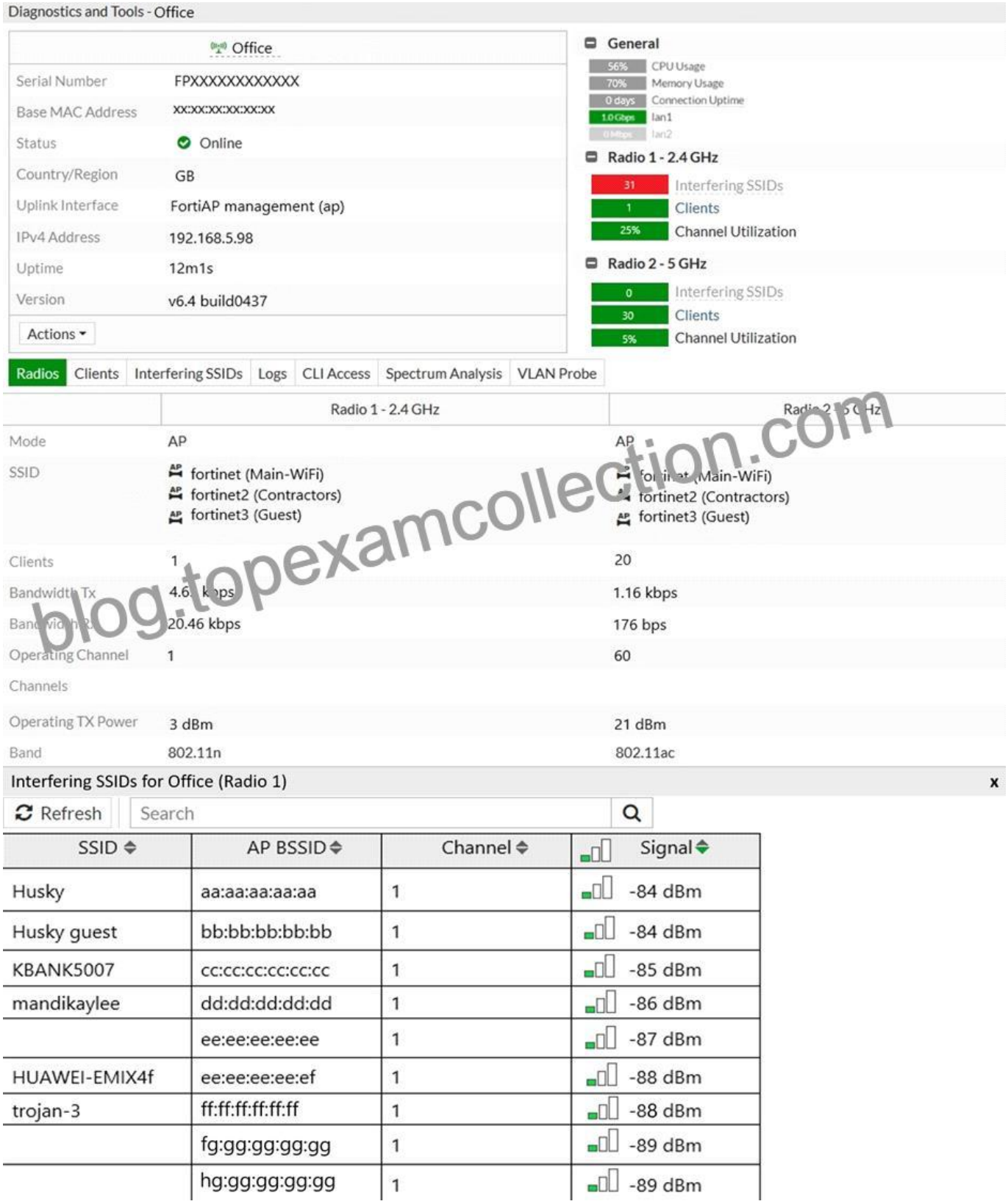
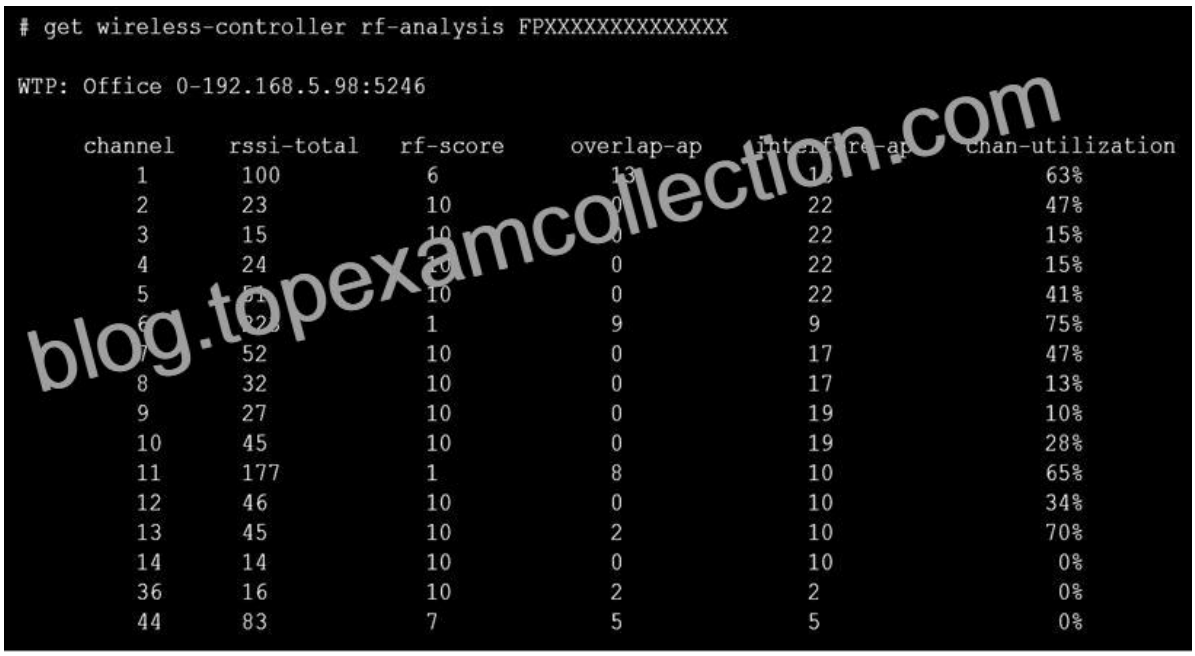


Exhibit C



```
# 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?
* Increase the transmission power of the AP radios
* Enable frequency handoff on the AP to band steer clients
* Reduce the number of wireless networks being broadcast by the AP
* Install another AP in the reception area to improve available bandwidth

NO.28 Which of the following is a requirement to generate analytic reports using on-site FortiPresence deployment?
* SQL services must be running
* Two wireless APs must be sending data
* DTLS encryption on wireless traffic must be turned off
* Wireless network security must be set to open

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.

NO.29 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?
* Configure the APs individually by overriding the settings in Managed FortiAPs

* Configure the controller for the correct country code for Germany
* Clone a suitable FortiAP profile and change the county code settings on the profile
* Create a new FortiAP profile and change the county code settings on the profile

NO.30 Which two phases are part of the process to plan a wireless design project? (Choose two.)
* Project information phase
* Hardware selection phase
* Site survey phase
* Installation phase

NO.31 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?
* Enable Locate WiFi clients when not connected in the relevant AP profiles.
* Enable Monitor channel utilization on the relevant AP profiles.
* Ensure that all allowed channels are enabled for the AP radios.
* Enable Radio resource provisioning on the relevant AP profiles.

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.

NO.32 Where in the controller interface can you find a wireless client’s upstream and downstream link rates?
* On the AP CLI, using the cw_diag ksta command
* On the controller CLI, using the diag wireless-controller wlac -d sta command
* On the AP CLI, using the cw_diag -d sta command
* On the controller CLI, using the WiFi Client monitor