Vendor: Fortinet

Exam Code: FCP_FWF_AD-7.4

Exam Name: FCP - Secure Wireless LAN 7.4 Administrator

Version: DEMO

QUESTION 1
What is the relationship between wireless channels and data transmission?

A. The wider the channel, the more data it can carry.
B. Data is transmitted over only one wireless channel at a time.
C. The more wireless channels, the more power consumption is required.
D. A wireless channel is allocated to transmit data unidirectionally.

Answer: A
Explanation:
A channel's bandwidth (e.g., 20 MHz vs. 40 MHz vs. 80 MHz) directly correlates to how many OFDM subcarriers it can support - more subcarriers mean higher aggregate throughput.

QUESTION 2
What protection does WPA3 wireless encryption provide over WPA2 for securing wireless networks?

A. WPA3 uses 128-bit session key size
B. WPA3 enforces only enterprise security mode
C. WPA3 addresses the KRACK vulnerability
D. WPA3 prevents legacy and deprecated wireless protocols from being used

Answer: C
Explanation:
WPA3 replaces the vulnerable four-way WPA2 handshake with SAE (Simultaneous Authentication of Equals), which provides robust forward secrecy and is not susceptible to the KRACK replay-attack flaws that affect WPA2. This ensures each session's keys cannot be recovered or reused by an attacker monitoring handshake messages.

QUESTION 3
A FortiAP device is connected directly to a FortiGate interface.

What discovery method will be used to provision the FortiAP device?

A. FortiGate discovers the FortiAP IP address from DHCP option 138.
B. FortiGate discovers the FortiAP through the received broadcast packets.
C. FortiAP discovers FortiGate by reviewing the vendor class value.
D. FortiAP discovers FortiGate by connecting to FortiLAN Cloud to verify its management license.

Answer: B
Explanation:
When a FortiAP and FortiGate share the same L2 network, the AP sends out a CAPWAP "discovery" broadcast (to 255.255.255.255) and the FortiGate listens for and replies to those broadcasts, automatically provisioning the AP without requiring DHCP option configuration.

QUESTION 4
Refer to the exhibits. User1 is part of the infrastructure department and connects to the ONBOARD wireless network using the credentials **user1**. However, the dynamic VLAN assignment is not working.

Which configuration step must you take to fix this issue?

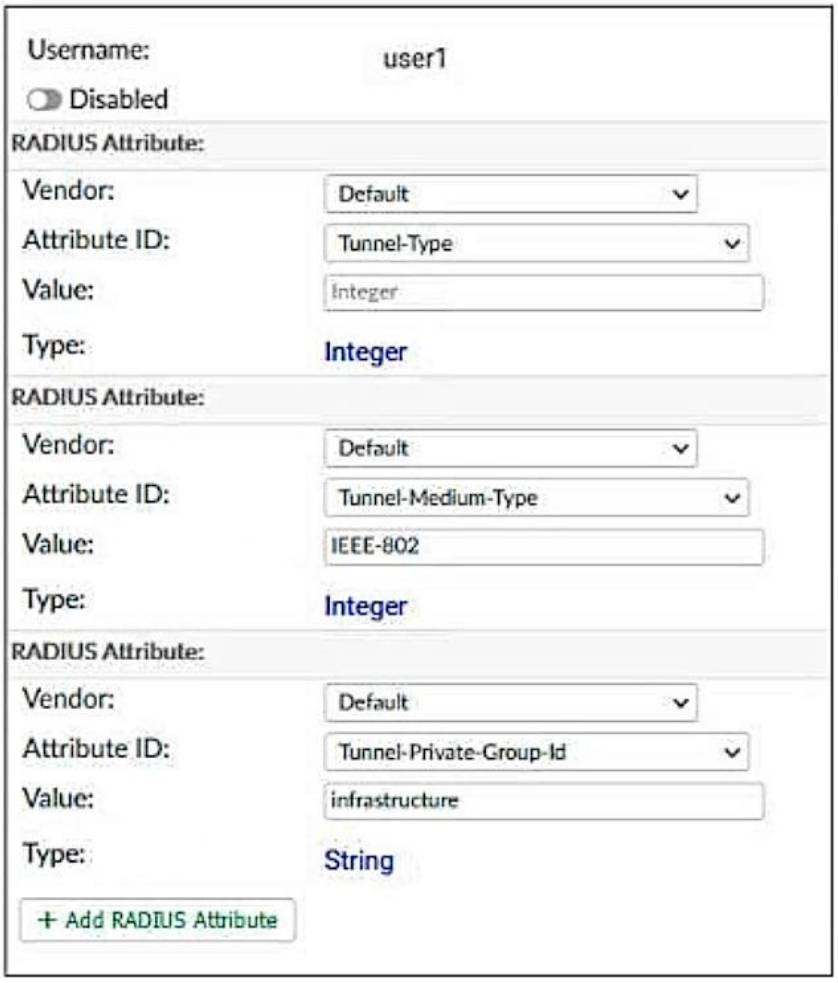
DHCP server settings

```
config system dhcp server
    edit 1
        set dns-service default
        set default-gateway 10.0.10.254
        set netmask 255.255.255.0
        set interface "WLAN01"
        config ip-range
            edit 1
                set start-ip 10.0.10.2
                set end-ip 10.0.10.100
            next
        end
    next
end
```

Wireless controller settings

```
config wireless-controller vap
    edit "WLAN01"
        set ssid "ONBOARD"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "FAC"
        set schedule "always"
        set dynamic-vlan enable
        config vlan-name
            edit "data"
                set vlan-id 100 200 300
            next
            edit "iot"
                set vlan-id 400
            next
        end
    next
end
```

RADIUS configuration



A. Disable the DHCP server on ONBOARD to allow VLAN assignment.
B. Add user1 in one of the VLAN names.
C. Update user1 RADIUS attributes to include a VLAN ID attribute ID.
D. Create a new VLAN name “infrastructure” with a VLAN ID associated with it.

Answer: D
Explanation:
For dynamic-VLAN assignment FortiGate matches the RADIUS Tunnel-Private-Group-Id string against the VLAN names you’ve configured under that SSID. Since you sent “infrastructure” but only have “data” and “iot” defined, you must add an “infrastructure” VLAN entry (with its VLAN ID) to the WLAN01 profile so the RADIUS attribute can map correctly.

QUESTION 5
Refer to the exhibits. FortiGate is pushing the POST parameters shown in the exhibit to the external captive portal server. The wireless client redirection fails because certificate validation occurred while loading the web page.

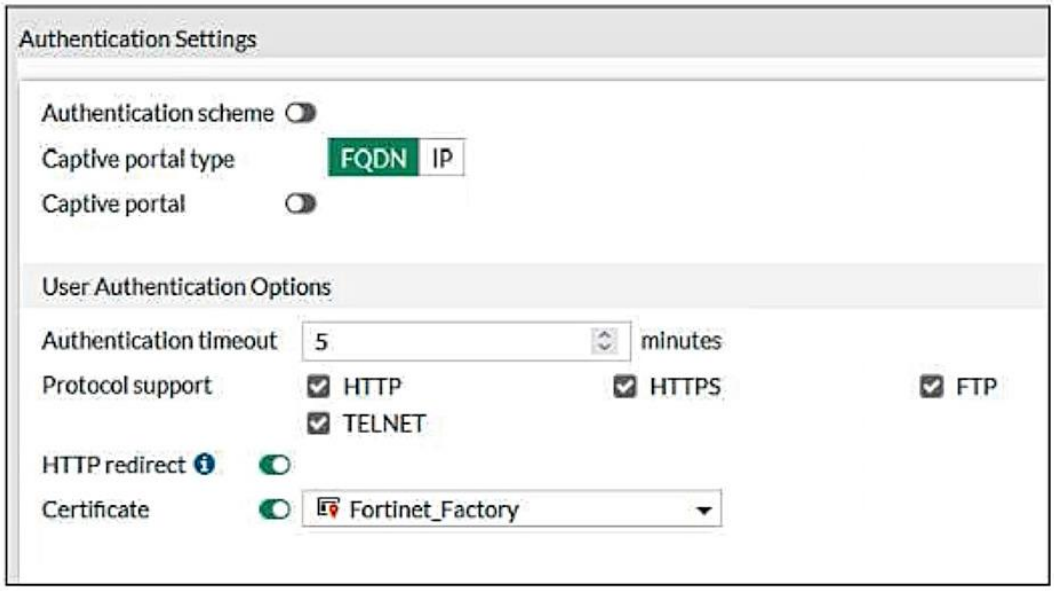
The wireless client browser uses the FortiGate self-signed certificate to access secured web pages. The SSID on FortiGate has the captive portal setting enabled.

What could cause the certification validation error on the wireless client?

Captive portal POST parameters

```
https://10.0.1.150/guests/login/?login&post=https://auth.trainingad.training.lab:1003/f
gtauth&magic=000a038293d1f411&usermac=b8:27:eb:d8:50:02&apmac=70:4c:a5:9d:0d:28&apip=10
.10.100.2&userip=10.0.3.1&ssid=Guest03&apname=FP231FTF20011555&bssid=70:4c:a5:9d:0d:30
```

Captive portal authentication settings



A. The FortiGate IP address in the POST parameters is using a numerical IP address.
B. The external server address is not the FQDN address.
C. The used credential is not embedded in the captive portal parameters.
D. The captive portal setting in the authentication setting is set to use FQDN as the captive portal type.

Answer: D
Explanation:
Because you've configured the portal to use an FQDN but the redirect URL (and certificate) is based on an IP address, the browser sees a host-name mismatch when validating the FortiGate's self-signed cert. Aligning the captive-portal type and the redirect URL (both via FQDN or both via IP) resolves the validation error.

QUESTION 6
Refer to the exhibits. The exhibits show the AP profile, the controller RF analysis output, and a diagnostic summary of the AP and neighboring APs.

The wireless 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.

Which configuration change is most likely to improve performance?

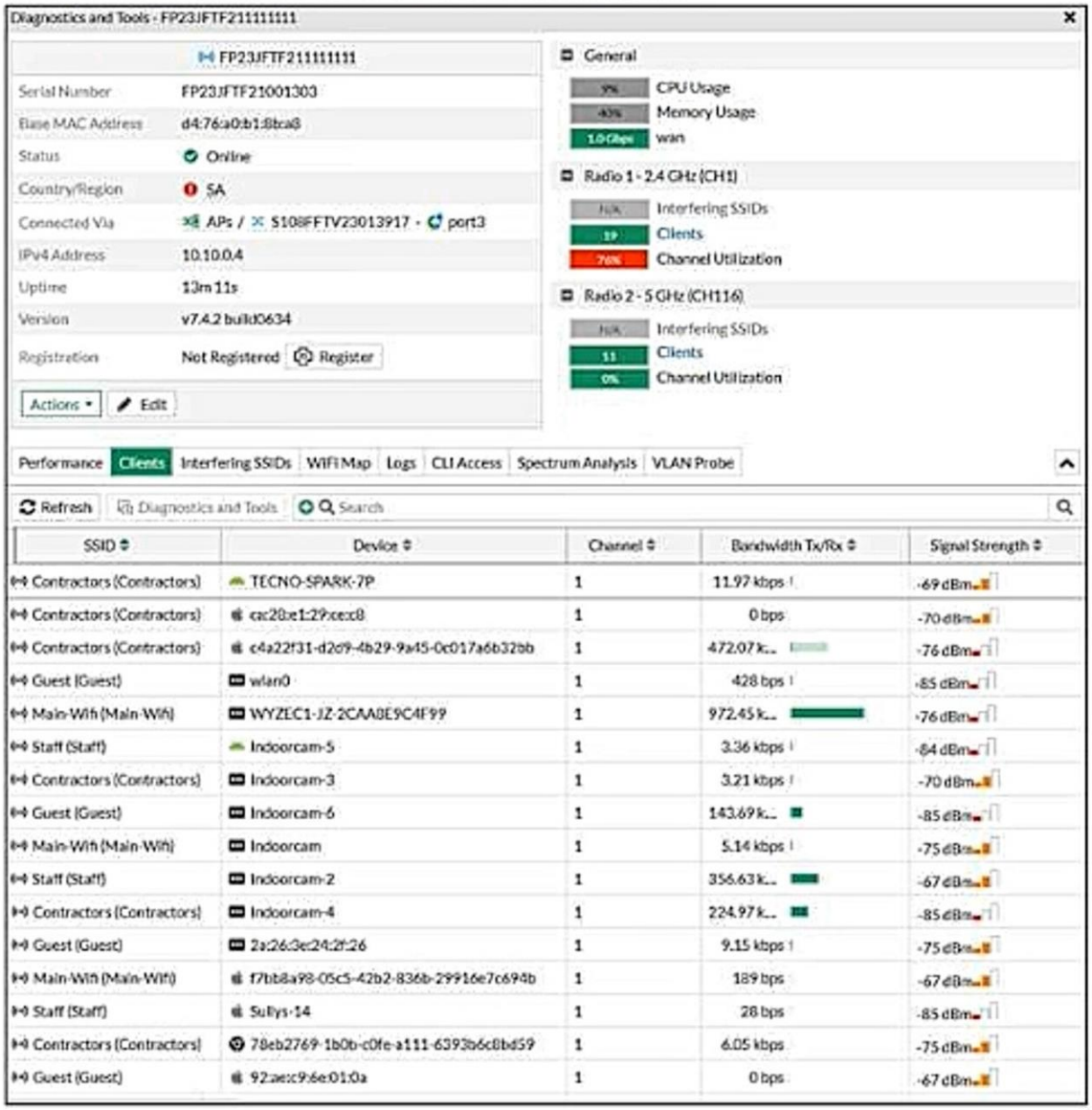
AP profile

```
config wireless-controller wtp-profile
    edit "Main networks - 23J"
        config platform
            set type 23JF
            set ddscan enable
        end
        set handoff-sta-thresh 55
        set ap-country SA
        set frequency-handoff enable
        config radio-1
            set band 802.11n-only
            set power-level 50
            set vap-all manual
            set vaps "Contractors" "Guest" "Main-Wifi" "Staff" "Students" "Wifi_IOT" "Wifi_POS"
        end
        config radio-2
            set band 802.11ac-only
            set channel-bonding 40MHz
            set power-level 60
            set vap-all manual
            set vaps "Contractors" "Main-Wifi" "Staff" "Students" "Wifi_IOT" "Wifi_POS"
        end
        config radio-3
            set mode monitor
            set wids-profile "default-wids-apscan-enabled"
        end
    next
end
```

The controller RF analysis output

```
61E-01 # get wireless-controller rf-analysis
WTP: FP23JFTF21111111  0-10.10.0.2:15246
     channel    rssi-total    rf-score     overlap-ap    interfere-ap chan-utilizaion
           1           275           1              8               7             91%
           2            73           8              0               9             80%
           3            49          10              0              11             62%
           4            80           7              5              11             54%
           5            45          10              1              11             69%
           6            77           8              2               8             49%
           7            55           9              2              14             65%
           8            24          10              0              14             57%
           9            29          10              0              12             58%
          10            59           9              1              11             61%
          11           180           1              9               9             48%
          12            43          10              0               7             38%
          13            19          10              0               7             58%
          14             8          10              0               7             49%
          36            26          10              2               2             39%
         100           249           1              3               3             89%
         116            72           8              2               2             68%
         149            44          10              3               3             54%
```

Diagnostic summary of the AP and neighboring APs



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

Answer: A
Explanation:
Every SSID (VAP) generates its own beacon and management frames, which on a heavily-utilized 2.4 GHz channel (91 % busy) adds significant overhead and cuts into airtime for client data. By cutting back to only the SSIDs needed in the reception area (for example, Guest and perhaps one additional SSID), you'll reduce beacon traffic and free up more of that already-scarce airtime for user throughput.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

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

★ Average **99.9%** Success Rate.

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

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

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

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

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

★ **Fast**, helpful support **24x7**.

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

10% Discount Coupon Code: **ASTR14**