Fortinet

Exam Questions FCP_FWF_AD-7.4

FCP - Secure Wireless LAN 7.4 Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

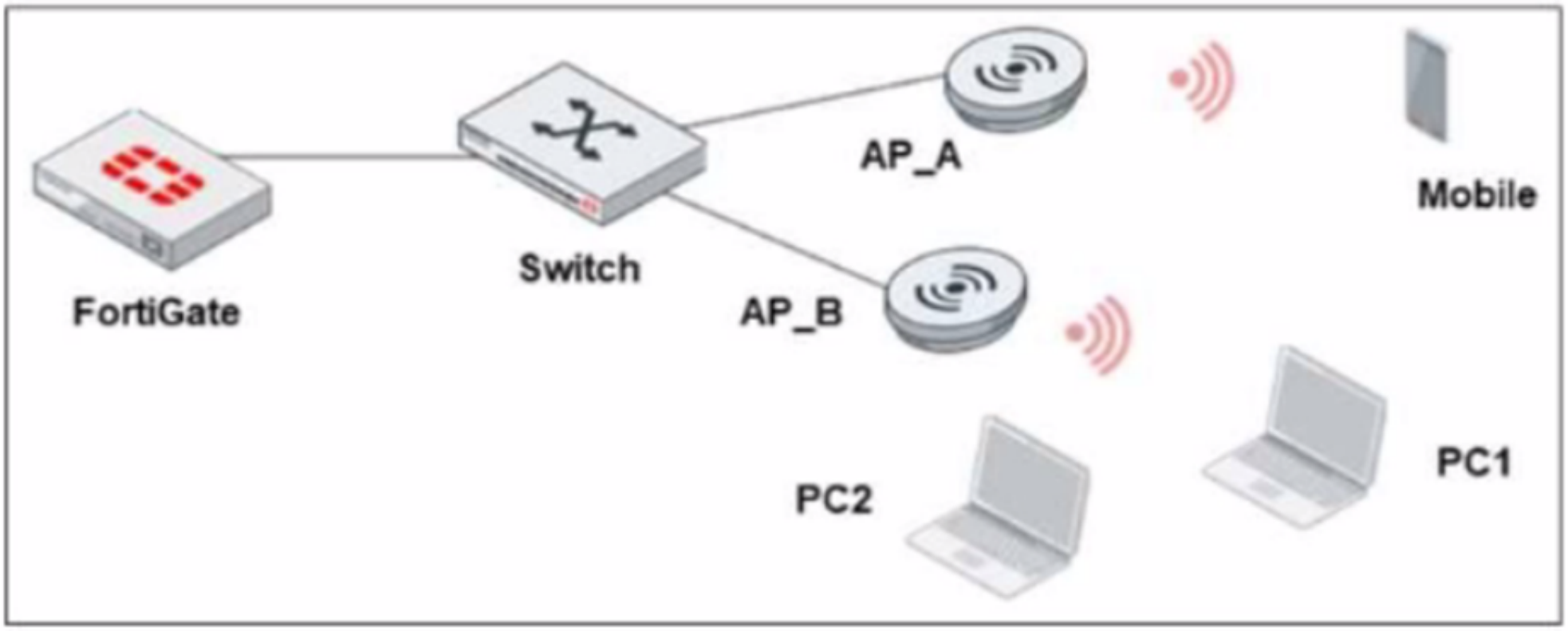
* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Refer to the exhibit.



A new security policy is made by the IT department to prevent direct communication between wireless stations There is one SSID configured in bridge mode
Which statement is correct as a plan of action to update the wireless network configuration?

A. Create unique SSIDs for each FortiAP device
B. Add an upstream layer 3 device on each FortiAP device
C. Block intra-SSID traffic on the wireless network
D. Drop all local traffic in the wireless network

Answer: C

Explanation:
Scenario:
The IT department wants to prevent direct communication between wireless stations.
There is one SSID configured in bridge mode (all clients on the same SSID/VLAN, directly bridging to the wired network).
Correct Action:
Block intra-SSID traffic (sometimes called ??client isolation?? or ??intra-SSID privacy??).
This feature prevents wireless clients connected to the same SSID from communicating directly with each other at Layer 2.
Each station can reach the network but cannot reach other wireless clients on the same SSID.
This is the industry-standard method to achieve the stated security goal in a wireless environment, especially in bridge mode.
Why Other Options Are Incorrect:
* A. Create unique SSIDs for each FortiAP device
Impractical and unnecessary for user isolation; users on the same SSID but different APs can still be isolated with intra-SSID blocking.
* B. Add an upstream layer 3 device on each FortiAP device
Overkill and not required; this does not directly solve intra-SSID traffic.
* D. Drop all local traffic in the wireless network
Too broad; you only want to prevent client-to-client communication, not all local traffic (such as traffic to the gateway).
Summary:
Block intra-SSID traffic is the intended and correct configuration to prevent wireless stations from communicating directly while sharing the same SSID in bridge mode.

NEW QUESTION 2
You plan to deploy a wireless network at various remote sites with no on-site IT available. The remote sites must have access points to broadcast the wireless networks You can manage the access points using any Fortinet control and management option
Which two items must you consider in addition to deploying the wireless network and enforcing Fortinet UTM on all wireless traffic? (Choose two.)

A. To install the access points designed to provide Fortinet UTM services
B. To power the access points with a UIM capable FortSwitch device
C. To deploy the SSIDs in bridge mode bridged to the access points subnet
D. To manage the access points by FortiLAN Cloud and create a tunnel between access points

Answer: AD

Explanation:
For remote sites with no on-site IT, you should:
A: Use APs that support Fortinet UTM (i.e., FortiAPs that can tunnel traffic back to a FortiGate for UTM enforcement).
D: Use cloud-based management (FortiLAN Cloud) and configure tunnel SSIDs so all traffic from the AP is sent back for security inspection at a central FortiGate.
B refers to PoE power but isn??t essential if APs can be powered in another way.
C (bridge mode to local subnet) would not allow centralized UTM enforcement unless local FortiGate is present.

NEW QUESTION 3
When enabling a Security Fabric connection on a FortiGate interface to manage FortiAP devices, which two types of CAPWAP communication channels are established between FortiGate and the FortiAP devices'? (Choose two)

A. Control channels
B. Data channels
C. Security channels
D. Fortlink channels

Answer: AB

Explanation:
When enabling a Security Fabric connection on a FortiGate interface to manage FortiAP devices, the following two types of CAPWAP (Control and Provisioning of Wireless Access Points) communication channels are established:
Control channels:
Correct. The control channel is used for management and control information between the FortiGate (controller) and FortiAP. This includes configuration, monitoring, and state updates.
Data channels:
Correct. The data channel carries client traffic between the FortiAP and FortiGate. This enables the FortiGate to apply security policies, content filtering, and other services to wireless client data.
Analysis of Other Options:
* C. Security channels:
There is no specific ??security channel?? in CAPWAP terminology.
* D. Fortlink channels:
FortLink is used for FortiSwitch management, not FortiAPs. CAPWAP is the protocol for FortiAP management.
References:
FortiOS 7.4 Administration Guide, Wireless Controller and CAPWAP sections: ??The communication between the FortiGate and FortiAP uses CAPWAP, which establishes both a control channel for management and a data channel for client traffic.??

NEW QUESTION 4
Which benefit does 802.1X authentication offer when securing a wireless network?

A. Authentication and authorization m enterprise networks
B. Allows administrators to gain elevated privilege to access resources
C. Makes wireless access at home protected and secured
D. Simplifies public Wi-Fi hotspots for guest access

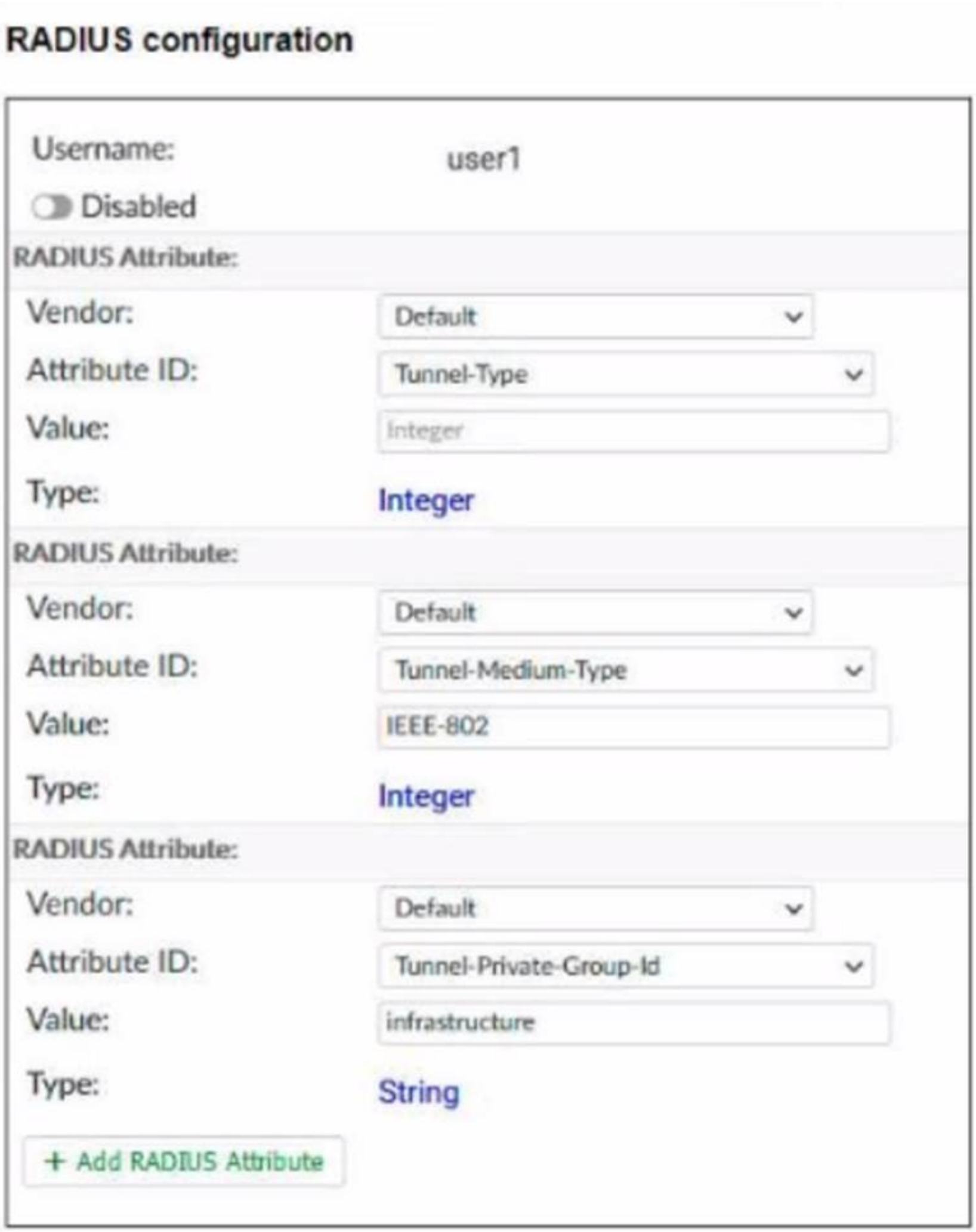
Answer: A

Explanation:
* 802.1 X is the standard for port-based network access control, widely used in enterprise Wi-Fi to:
Authenticate users and devices before granting access to the network.
Authorize network access (optionally placing users into specific VLANs).
It is not for home Wi-Fi (C), does not provide admin privilege (B), and is more complex than open guest Wi- Fi (D).

NEW QUESTION 5
Refer to the exhibit.

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
```



User1 is part of the infrastructure department and connects to the ONBOARD wireless network using the credentials uteri. However, the dynamic VLAN assignment is not working
Which configuration step must you take to fix this issue?

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: C

Explanation:
Analysis of the Exhibits and Scenario:
The DHCP server configuration is correct for dynamic assignment within a specified IP range for the interface ??WLAN01??.
The RADIUS configuration for user1 includes:
Tunnel-Type (should be set to VLAN, but value is missing)
Tunnel-Medium-Type (set to IEEE-802, which is correct for Ethernet/WiFi) Tunnel-Private-Group-Id (set to ??infrastructure?? as a string)
The problem described: Dynamic VLAN assignment is not working for user1.
How Dynamic VLAN Assignment Works in 802.1X/EAP (with FortiGate/FortiAP):
When a user authenticates, the RADIUS server returns attributes specifying the VLAN that should be assigned.
The critical attributes are:
Tunnel-Type (must be set to value ??VLAN??, which is integer 13) Tunnel-Medium-Type (must be ??IEEE-802??, integer 6)

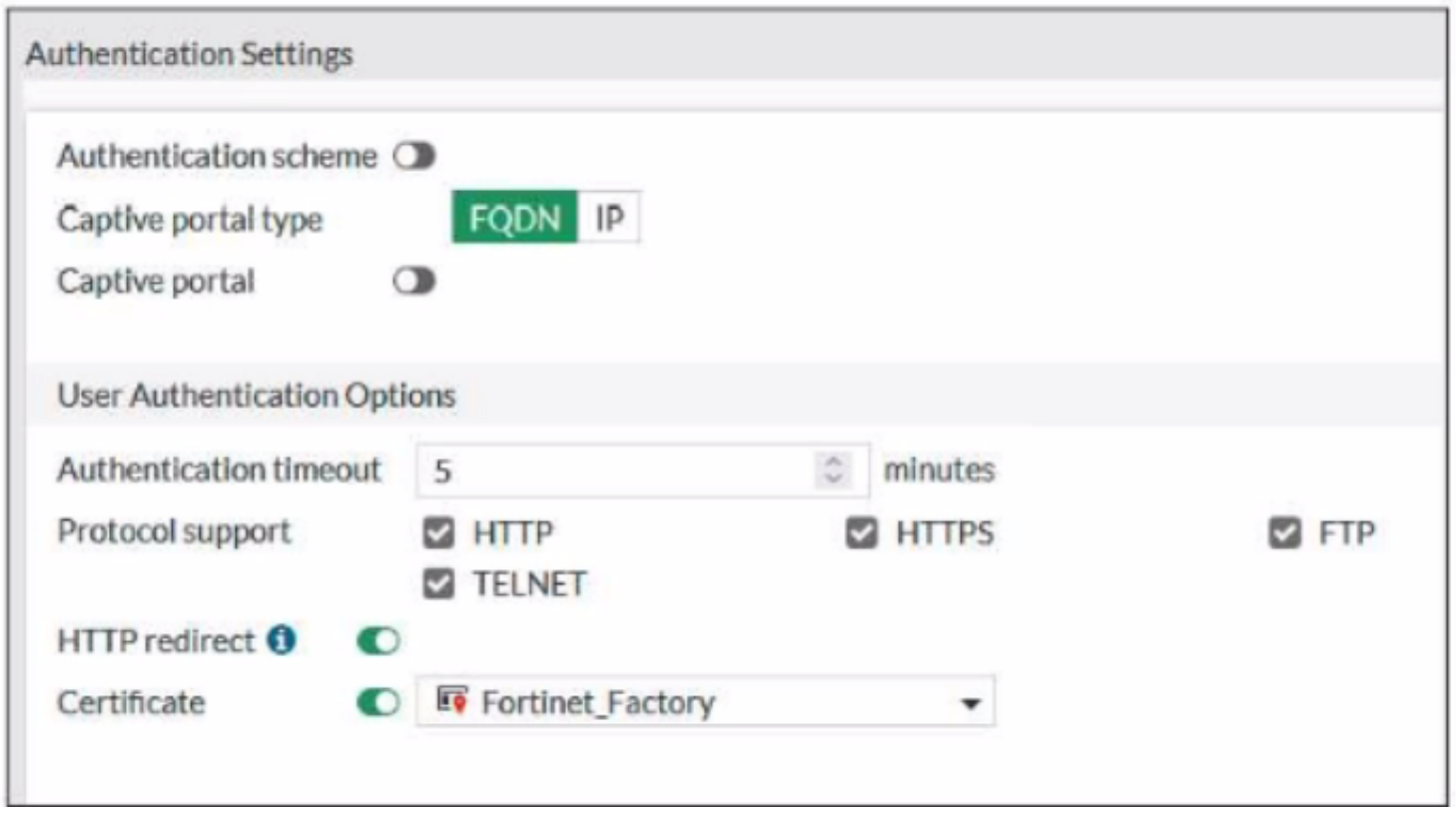
Tunnel-Private-Group-Id (can be the VLAN name or VLAN ID, depending on your configuration) Problem in the Exhibit:
The Tunnel-Type value is missing! It must be set to 13 (for VLAN).
The Tunnel-Medium-Type and Tunnel-Private-Group-Id are correctly set. Corrective Action:
Update user1??s RADIUS attributes so that Tunnel-Type is set to the correct value for VLAN (integer 13).
Without this, FortiGate/FortiAP will not know to interpret the returned VLAN name or ID for dynamic assignment.
Review of Options:
Disable the DHCP server on ONBOARD to allow VLAN assignment. Irrelevant; DHCP server presence does not affect dynamic VLAN assignment. Add user1 in one of the VLAN names
This is not how dynamic VLAN assignment works. The RADIUS response must include the correct VLAN assignment.
Update user1 RADIUS attributes to include a VLAN ID attribute ID
Correct. You must set Tunnel-Type (13) and possibly provide the VLAN ID in Tunnel-Private-Group-Id. Create a new VLAN name infrastructure' with a VLAN ID associated with it
Not the root cause; you must first ensure the correct attributes are present in the RADIUS response. Summary:
The missing ??Tunnel-Type?? attribute value is the reason dynamic VLAN assignment is not working. The correct configuration requires setting Tunnel-Type = 13 (VLAN) for user1 in the RADIUS server.

NEW QUESTION 6
Refer to the exhibits.

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



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

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:
Scenario Analysis:
The wireless client is redirected to a captive portal for authentication.
The authentication settings (see second exhibit) show:
Captive portal type: FQDNis selected.
Certificate:Fortinet_Factory(the default self-signed certificate).
The browser is reporting acertificate validation errorwhen the redirection to the captive portal occurs.
Certificate Validation and Captive Portals:
When FQDN is used for captive portal redirection, the browser expects the SSLcertificate to be valid for the FQDN (e.g., ??captive.company.com??).
If the certificate isself-signedor doesnot match the FQDN(common when using the Fortinet factory default certificate), the browser will trigger a certificate error.
This is a common issue when FQDN-based portals are used without apublicly trusted certificate matching the FQDN.
Option Analysis:
* A. The FortiGate IP address in the POST parameters is using a numerical IP address
Not relevant; the browser validates the page being loaded, not the POST parameters.
* B. The external server address is not the FQDN address
In this case, the external captive portal URLisusing FQDN, as set in the authentication setting.
* C. The used credential is not embedded in the captive portal parameters

Credential handling is not related to certificate errors; it would result in login/authentication failures, not browser SSL warnings.
* D. The captive portal setting in the authentication setting is set to use FQDN as the captive portal type
Correct.When FQDN is used, the SSL certificate presented must be trusted and match the FQDN. The factory certificate will not match (it is not publicly trusted), so clients will see a validation error.
Summary:
Certificate validation fails because the captive portal is accessed via FQDN, but the FortiGate presents its self-signed factory certificate, which does not match the FQDN or is not trusted by browsers.

NEW QUESTION 7
Refer to the exhibit.

An administrator authorizes two FortiAP devices connected to this wireless controller However, one FortiAP is not able to broadcast the SSIDs. What must the administrator do to fix the issue?

A. Enable the radios on the FAP23JF FortiAP profile.
B. Replace the FortiAP device model to match the other device
C. Disable the override setting on the FortiAP that is preventing it from broadcasting SSIDs
D. Assign the FAP231F FortiAP profile to the problematic FortiAP device

Answer: A

Explanation:
Comprehensive Detailed Step by Step Explanation from all your Knowledge and Guides availableExhibit Analysis:
The screenshot displays two FortiAPs (FP231FT and FP23JFT) in the wireless controller??s managed APs list. Both APs are online and connected via APs.
FP231FT shows active SSIDs (??All Tunnel Mode SSIDs??) and has 11 clients connected. FP23JFT shows ??N/A?? for all SSIDs and ??0?? clients.
Diagnosis:
??N/A?? for SSIDs on FP23JFT clearly indicates it is not broadcasting any SSID.
Both APs are running the same OS version and have their respective FortiAP profiles assigned. Evaluating the Options:
* A. Enable the radios on the FAP23JF FortiAP profile.
Correct: If the radios (2.4GHz/5GHz) are disabled in the FortiAP profile, the AP will not broadcast any SSID, resulting in ??N/A?? and ??0 clients??. This is a common issue seen in FortiOS Wireless LAN management.
This matches the symptom, as the AP is online (communicating with the controller), but has no active radio (hence, no SSID is broadcasted).
* B. Replace the FortiAP device model to match the other device.
Incorrect. FortiOS supports different models in the same deployment, as long as the correct profile is applied.
* C. Disable the override setting on the FortiAP that is preventing it from broadcasting SSIDs.
Misleading. Unless an override has specifically disabled SSID broadcasting, this is not directly indicated by the screenshot. Usually, radio disabled at profile is the root cause.
* D. Assign the FAP231F FortiAP profile to the problematic FortiAP device.
Incorrect. The correct profile (FAP23JF) is already assigned to FP23JFT; assigning a mismatched profile can cause more issues and is not best practice.
Guide Reference & Reasoning:
FortiOS Administration Guide – Wireless Section:
When an AP is online but SSIDs are not broadcasted and ??N/A?? appears for radio slots, it strongly points to the radios being disabled in the FortiAP profile (see Wireless Controller > Managed FortiAPs).
The guide explains that ??If the radios are disabled in the profile, the AP will not broadcast any SSID. To resolve, enable the radios (2.4GHz, 5GHz) in the FortiAP profile and reapply or reboot the AP??.
FortiAP Profile Settings:
Go to WiFi & Switch Controller > FortiAP Profiles. Edit the FAP23JF profile.
Check both ??Radio 1?? and ??Radio 2?? (enable if disabled). Save the changes and ensure the profile is pushed to the AP. Typical Steps to Fix:
Log into the FortiGate.
Navigate to WiFi & Switch Controller > FortiAP Profiles. Edit the FAP23JF profile.
Under the radio settings, ensure both radios are set to ??Enable??.
Apply the changes.
The AP will now broadcast the SSIDs as configured. Summary:
The problem is caused by disabled radios in the FAP23JF FortiAP profile. Enabling the radios in the profile will allow the AP to start broadcasting SSIDs.
Final Answer A. Enable the radios on the FAP23JF FortiAP profile.

NEW QUESTION 8
Which two statements are correct about FortiAP and rogue APs? (Choose two.)

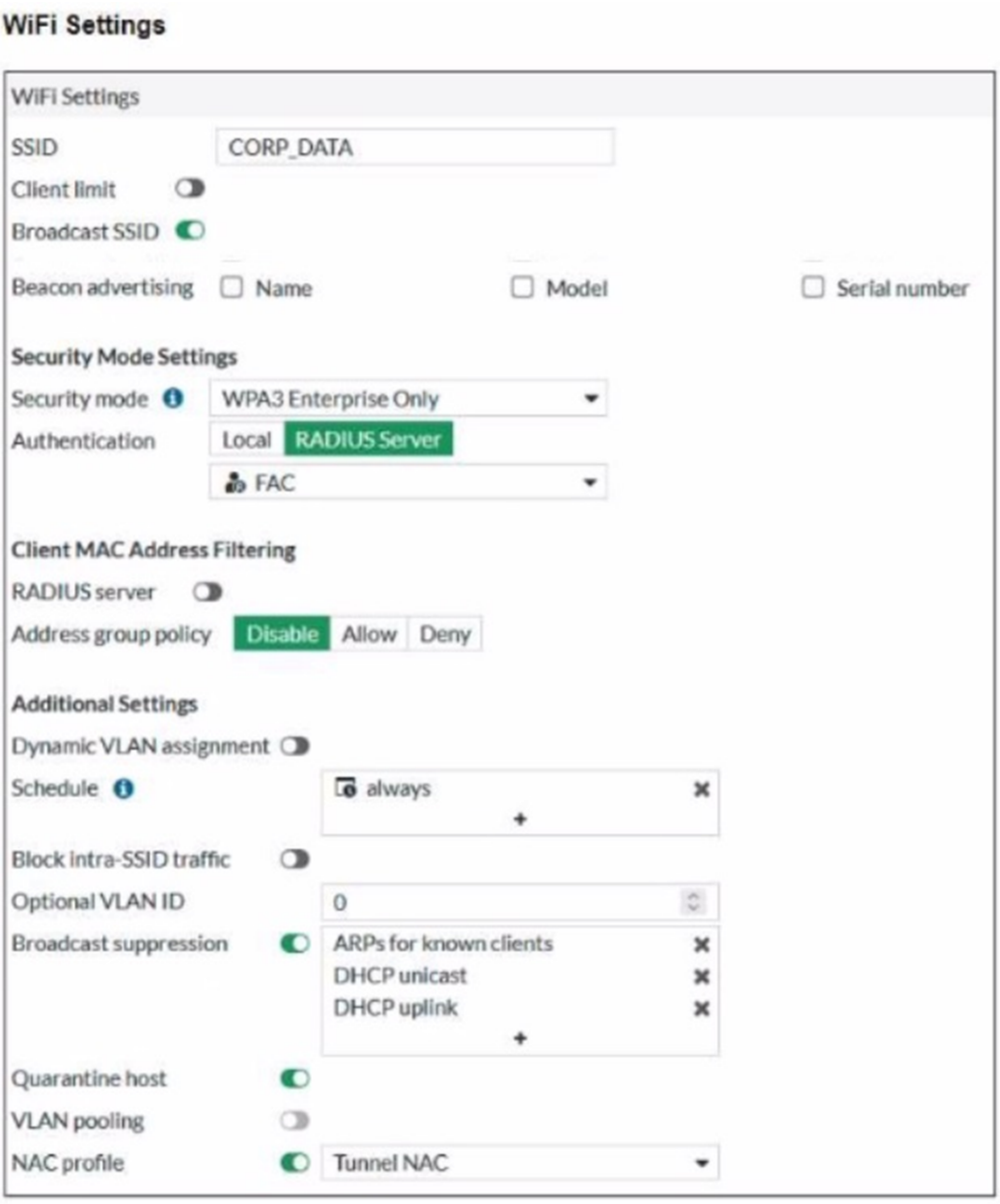
A. FortiAP offers automatic suppression of rogue APs when broadcasting SSIDs
B. FortiAP scans rogue APs in the background while broadcasting SSIDs
C. FortiAP detects rogue APs on dedicated monitoring radios
D. FortiAP suppresses detected rogue APs manually

Answer: BC

Explanation:

FortiAP and Rogue AP Detection: Background Scanning:
FortiAPs can perform background scanning for rogue APs while actively servicing clients (broadcasting SSIDs). This means they periodically switch from client service to scan the air for unauthorized APs.
This enables detection of threats without a dedicated radio, using periodic scans on service radios. Manual Suppression:
Suppression of rogue APs (for example, sending de-auth frames to clients of a rogue) must be triggered manually by an administrator from the FortiGate/FortiAP interface.
Automatic Suppression:
FortiAPs do NOT offer automatic suppression of rogue APs by default. Suppression is an explicit administrative action.
Dedicated Monitoring Radios:
Some APs (higher-end models) may have dedicated radios, but this is not the case for all FortiAPs; background scanning is the standard.
Option Breakdown:
* A. FortiAP offers automatic suppression of rogue APs when broadcasting SSIDs Incorrect. Suppression is manual.
* B. FortiAP scans rogue APs in the background while broadcasting SSIDs Correct. Background scanning is supported.
* C. FortiAP detects rogue APs on dedicated monitoring radios
Incorrect for most deployments. Dedicated monitoring radios are available only in some models.
* D. FortiAP suppresses detected rogue APs manually Correct. Manual suppression is available via the management interface.

NEW QUESTION 9
Refer to the exhibit.



FortiGate sends logs to FortiAnalyzer using the default settings to report security events for all wireless stations as part of the Security Fabric configuration
Which security action will FortiGate take when it detects a compromised wireless station in the CORP_DATASSlD?
A. CORP_DATA is in NAC mode and onboards compromised stations for a period until malicious activity stops
B. FortiGate disassociates compromised stations and prevents them from connecting again
C. FortiAnalyzer generates security reports to inform security operations to further Investigate the compromised stations
D. FortiAP devices broadcasting CORP_DATA wireless network place compromised stations in quarantine

A.

Answer: A

NEW QUESTION 10
How can you find the upstream and downstream link rates of a wireless client connected to a FortiAP?

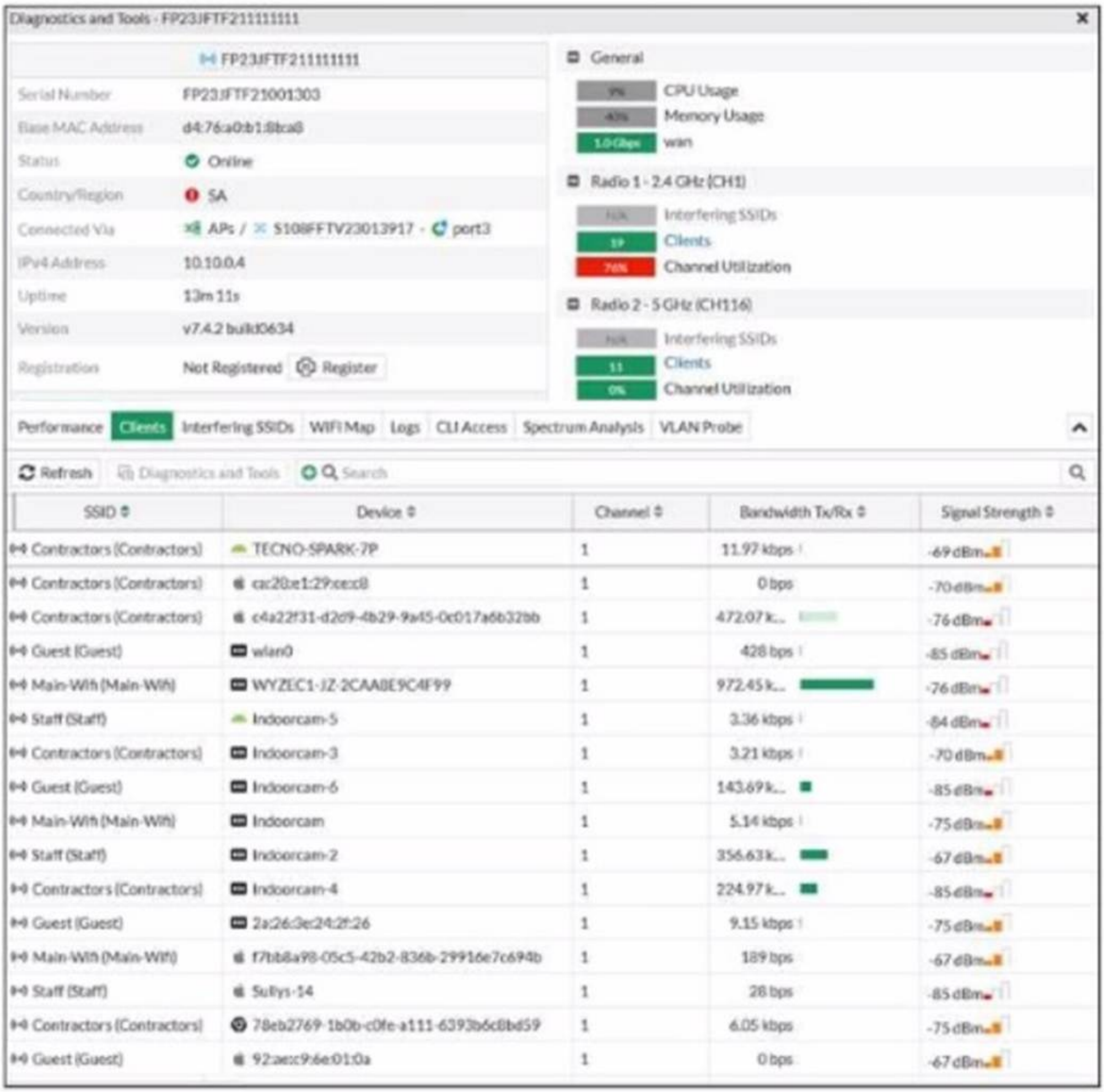
A. On the FortiGate GUI using the WiFi Client monitor
B. On the FortiAP CLI using the cw_diag ksta command
C. On the FortiGate CL! using the diagnose wireless-controller wlac -d sta command
D. On the FortiAP CLI using the cw_diag -d sea command

Answer: B

NEW QUESTION 10
Refer to the exhibits.

```
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



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 loT devices Users connecting to the guest network located in the reception area are reporting stow performance
Which configuration change is most likely to improve performance?

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:
Analysis of Exhibits:
RF Analysis:
Channel 1 (2.4 GHz) shows very high utilization (91%) and significant overlap/interference from other APs (8 overlap-AP, 7 interfere-AP).
Channel utilization on 2.4 GHz is very high, indicating congestion and contention.
AP Diagnostic Summary:
Radio 1 (2.4 GHz):
Channel Utilization: 78%
Interfering SSIDs: 18

A long list of clients and many SSIDs being broadcast on Channel 1.
Radio 2 (5 GHz):
Channel Utilization: 0% (much lower usage; likely not all clients or SSIDs are using it).
SSID List:
Multiple SSIDs are being broadcast by the AP, which increases management overhead (beacon /probe traffic) and reduces airtime for actual data.
Problem Symptoms:
Guest users in the reception area (on 2.4 GHz, channel 1) are experiencing slow performance.
Option Analysis:
* A. Reduce the number of SSIDs being broadcast by the reception AP
Correct.
Each SSID adds additional management overhead (beacons, probes) that consume airtime on already congested 2.4 GHz channels.
Reducing the number of SSIDs frees up airtime for actual client data, which can improve throughput and reduce latency, especially in high-density environments with high channel utilization.
This is a recommended best practice for optimizing Wi-Fi performance in congested environments.
* B. Enable frequency handoff on the AP to band steer clients
Helpful if clients support 5 GHz, but not all client devices (especially IoT/guests) do; with such high channel utilization, this is a secondary optimization.
* C. Increase the transmission power of the AP radios
This can make interference worse and does not solve airtime congestion; it may also increase contention with neighboring APs.
* D. Install another AP in the reception area to improve available bandwidth
Adding more APs on congested channels can actually increase interference and may not help unless channel planning and SSID management are also addressed.
Summary:
Reducing the number of SSIDs is the most direct, configuration-based action that will improve available airtime and performance for clients in a congested, high-utilization environment like the one shown in the exhibits.

NEW QUESTION 13
.....

Relate Links

100% Pass Your FCP_FWF_AD-7.4 Exam with Exambible Prep Materials

https://www.exambible.com/FCP_FWF_AD-7.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/