Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

NSE7_LED-7.0 Dumps
NSE7_LED-7.0 Braindumps
NSE7_LED-7.0 Real Questions
NSE7_LED-7.0 Practice Test
NSE7_LED-7.0 Actual Questions

PASS

## Fortinet

# NSE7_LED-7.0

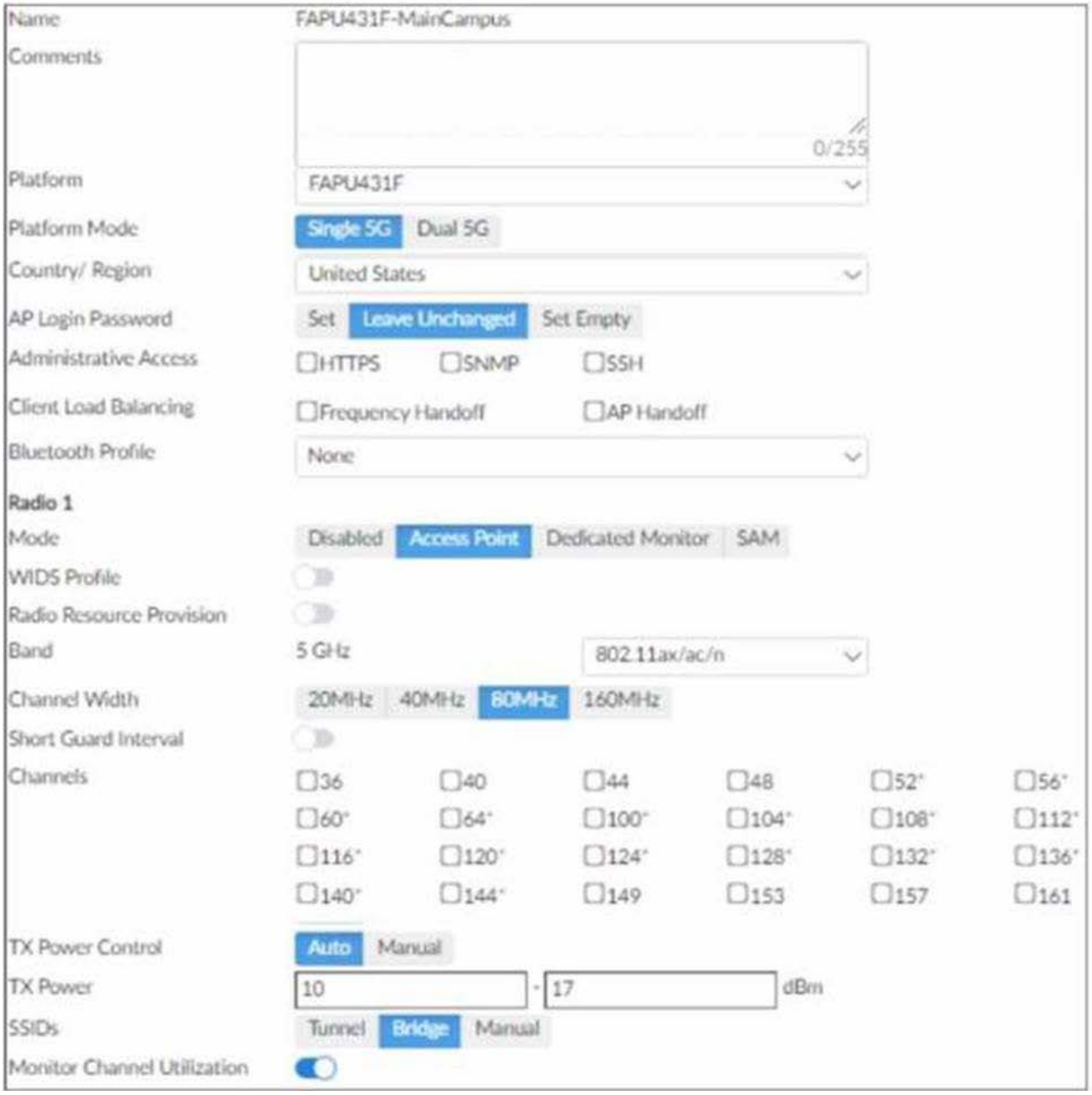
*NSE 7 - LAN Edge 7.0*

## Question: 86

Refer to the exhibits

SSID Profiles


AP Profile




The exhibits show the wireless network (VAP) SSID profiles defined on FortiManager and an AP profile assigned to a

group of APs that are supported by FortiGate None of the APs are broadcasting the SSlDs defined by the AP profile

Which changes do you need to make to enable the SSIDs to broadcast?

A. In the SSIDs section enable Tunnel
B. Enable one channel in the Channels section
C. Enable multiple channels in the Channels section and enable Radio Resource Provision
D. In the SSIDs section enable Manual and assign the networks manually

**Answer: B**

Explanation:

According to the FortiManager Administration Guide1, âTo enable the SSID, you must select at least one channel for the radio. If no channels are selected, the SSID will not be enabled.â Therefore, enabling one channel in the Channels section will allow the SSIDs to broadcast

## Question: 87

Which two statements about the guest portal on FortiAuthenticator are true? (Choose two.)

A. Each remote user on FortiAuthenticator can sponsor up to 10 guest accounts
B. Administrators must approve all guest accounts before they can be used
C. The guest portal provides pre and post-log in services
D. Administrators can use one or more incoming parameters to configure a mapping rule for the guest portal

**Answer: A,C,D**

Explanation:

According to the FortiAuthenticator Administration Guide2, âThe guest portal provides pre and post-log in services for users (such as password reset and token registration abilities), and rules and replacement messages can be configured.â Therefore, option C is true. The same guide also states that âAdministrators can use one or more incoming parameters to configure a mapping rule for the guest portal.â Therefore, option D is true. Option A is false because remote users can sponsor any number of guest accounts, as long as they do not exceed the maximum number of guest accounts allowed by the license. Option B is false because administrators can choose to approve or reject guest accounts, or enable auto-approval.

## Question: 88

Refer to the exhibit.

```
config wireless-controller wtp-profile
    edit "Main Networks - FAP-320C"
        set comment "Profile with standard networks"
        config platform
            set type 320C
        end
        set wan-port-mode wan-only
        set led-state enable
        set dtls-policy clear-text
        set max-clients 0
        set handoff-rssi 30
        set handoff-sta-thresh 30
        set handoff-roaming enable
        set ap-country GB
        set ip-fragment-preventing tcp-mss-adjust
        set tun-mtu-uplink 0
        set tun-mtu-downlink 0
        set split-tunneling-acl-path local
        set split-tunneling-acl-local-ap-subnet enable
        config split-tunneling-acl
            edit 1
                set dest-ip 192.168.5.0 255.255.255.0
            next
        end
        set allowaccess https ssh
        set login-passwd-change yes
        set lldp disable
```

Exhibit.

```
        config radio-1
            set mode ap
            set band 802.11n,g-only
            set protection-mode disable
            unset powersave-optimize
            set amsdu enable
            set coexistence enable
            set short-guard-interval disable
            set channel-bonding 20MHz
            set auto-power-level disable
            set power-level 100
            set dtim 1
            set beacon-interval 100
            set rts-threshold 2346
            set channel-utilization enable
            set spectrum-analysis disable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set max-clients 0
            set max-distance 0    next
config wireless-controller vap
    edit "Corporate"
        set ssid "Corporate"
        set passphrase ENC XXXX
        set schedule "always"
        set quarantine disable
    next
end
```

Refer to the exhibits

In the wireless configuration shown in the exhibits, an AP is deployed in a remote site and has a wireless network

(VAP) called Corporate deployed to it

The network is a tunneled network however clients connecting to a wireless network require access to a local printer Clients are trying to print to a printer on the remote site but are unable to do so.

Which configuration change is required to allow clients connected to the Corporate SSID to print locally?

A. Configure split-tunneling in the vap configuration
B. Configure split-tunneling in the wtp-profile configuration
C. Disable the Block Intra-SSID Traffic (intra-vap-privacy) setting on the SSID (VAP) profile
D. Configure the printer as a wireless client on the Corporate wireless network

## Answer: A

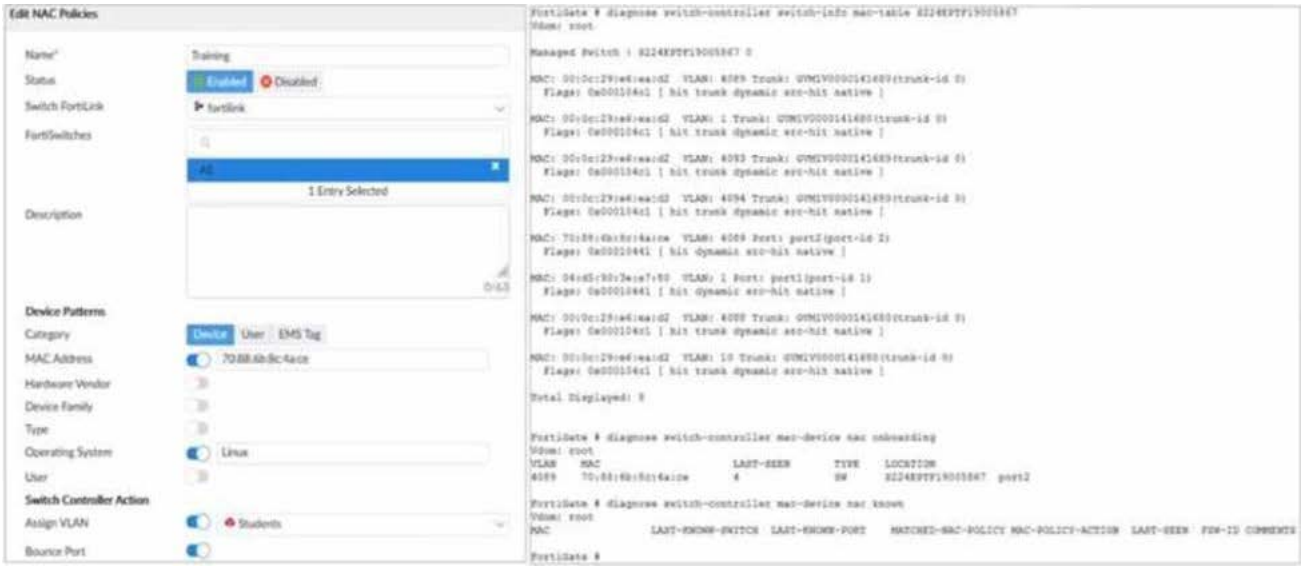
Explanation:

According to the Fortinet documentation1, âSplit tunneling allows you to specify which traffic is tunneled to the FortiGate and which traffic is sent directly to the Internet. This can improve performance and reduce bandwidth usage.â Therefore, by configuring split-tunneling in the vap configuration, you can allow the clients connected to the Corporate SSID to access both the corporate network and the local printer. Option B is incorrect because split-tunneling is configured at the vap level, not the wtp-profile level. Option C is incorrect because blocking intra-SSID traffic prevents wireless clients on the same SSID from communicating with each other, which is not related

to accessing a local printer. Option D is unnecessary and impractical because the printer does not need to be a wireless client on the Corporate wireless network to be accessible by the clients.

## Question: 89

Refer to the exhibit.




Examine the FortiManager configuration and FortiGate CLI output shown in the exhibit

An administrator is testing the NAC feature The test device is connected to a managed FortiSwitch device {S224EPTF19"537)onpOrt2

After applying the NAC policy on port2 and generating traffic on the test device the test device is not matching the NAC policy therefore the test device remains m the onboarding VLAN

Based on the information shown in the exhibit which two scenarios are likely to cause this issue? (Choose two.)

A. Management communication between FortiGate and FortiSwitch is down
B. The MAC address configured on the NAC policy is incorrect
C. The device operating system detected by FortiGate is not Linux
D. Device detection is not enabled on VLAN 4089

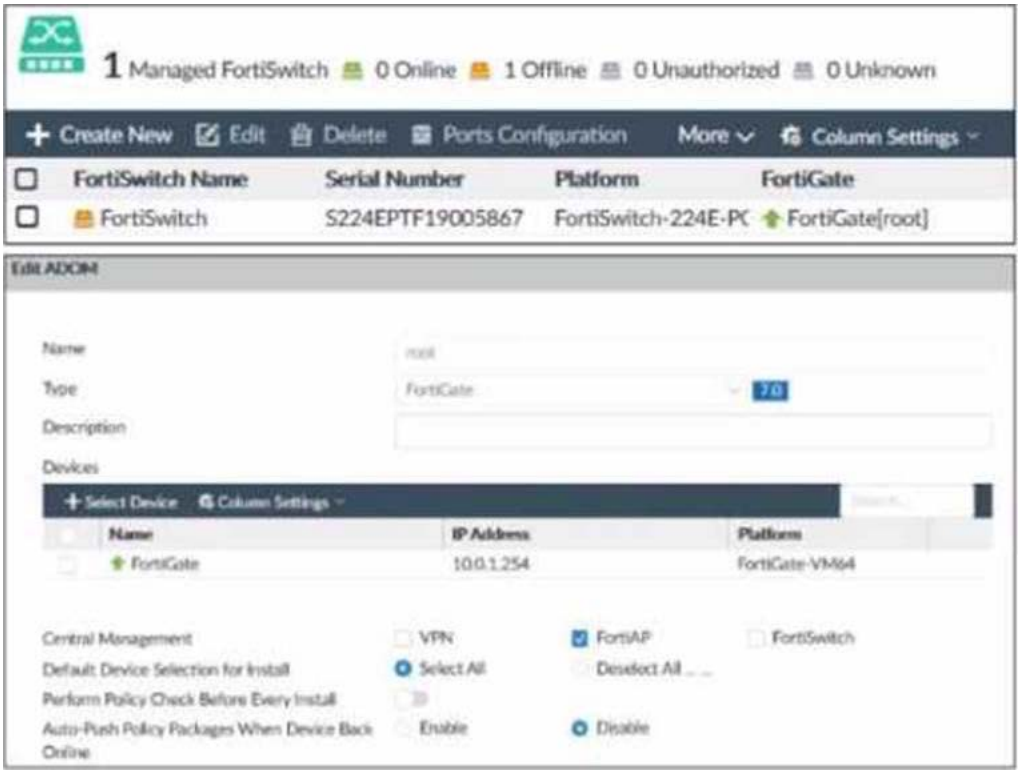
**Answer: A,B**

Explanation:

According to the FortiManager configuration, the NAC policy is set to match devices with the MAC address of 00:0c:29:6a:2b:3c and the operating system of Linux. However, according to the FortiGate CLI output, the test device has a different MAC address of 00:0c:29:6a:2b:3d. Therefore, option B is true. Option A is also true because the FortiSwitch device status is shown as down, which means that the management communication between FortiGate and FortiSwitch is not working properly. This could prevent the NAC policy from being applied correctly. Option C is false because the device operating system detected by FortiGate is Linux, which matches the NAC policy. Option D is false because device detection is enabled on VLAN 4089, as shown by the command âconfig switch-controller vlanâ.

## Question: 90

Refer to the exhibit.




Examine the FortiManager information shown in the exhibit

Which two statements about the FortiManager status are true" (Choose two)

A. FortiSwitch manager is working in per-device management mode
B. FortiSwitch is not authorized
C. FortiSwitch manager is working in central management mode
D. FortiSwitch is authorized and offline

**Answer: A,C,D**

Explanation:

According to the FortiManager Administration Guide, âCentral management mode allows you to manage all FortiSwitch devices from a single interface on the FortiManager device.â Therefore, option C is true because the exhibit shows that the FortiSwitch manager is enabled and the FortiSwitch device is managed by the FortiManager device. Option D is also true because the exhibit shows that the FortiSwitch device status is offline, which means that it is not reachable by the FortiManager device, but it is authorized, which means that it has been added to the FortiManager device. Option A is false because per-device management mode allows you to manage each FortiSwitch device individually from its own web-based manager or CLI, which is not the case in the exhibit. Option B is false because the FortiSwitch device is authorized, as explained above.

## Question: 91

An administrator has configured an SSID in bridge mode for corporate employees All APs are online and provisioned using default AP profiles Employees are unable to locate the SSID to conned

Which two configurations can the administrator verify? (Choose two)

A. Verify that the broadcast SSID option is enabled in the SSID configuration
B. Verify that the Block Intra-SSID Traffic (intra-vap-privacy) option in the SSID configuration is disabled
C. Verify that the SSID to an AP group that should be broadcasting the SSID is applied
D. Verify that the SSID is manually applied on AP profiles for both 2 4 GHz and 5 GHz radios

**Answer: A,C**

Explanation:

According to the FortiAP Configuration Guide1, âTo enable the SSID, you must select at least one channel for the radio. If no channels are selected, the SSID will not be enabled. You must also enable Broadcast SSID.â Therefore, option A is true because the broadcast SSID option allows the SSID to be visible to wireless clients. Option C is also true because the SSID must be applied to an AP group that contains the APs that should be broadcasting the SSID. According to the same guide1, âYou can create AP groups and assign them to different locations or departments. You can then apply different settings, such as SSIDs, to each group.â Option B is false because blocking intra-SSID traffic prevents wireless clients on the same SSID from communicating with each other, which is not related to broadcasting the SSID. Option D is false because the SSID can be applied to an AP group or a global profile, which will automatically apply to all APs, without manually configuring each AP profile.

## Question: 92

What is the purpose of enabling Windows Active Directory Domain Authentication on FortiAuthenticator?

A. It enables FortiAuthenticator to use Windows administrator credentials to perform an LDAP lookup for a user search
B. It enables FortiAuthenticator to use a Windows CA certificate when authenticating RADIUS users
C. It enables FortiAuthenticator to import users from Windows AD
D. It enables FortiAuthenticator to register itself as a Windows trusted device to proxy authentication using Kerberos

## Answer: D

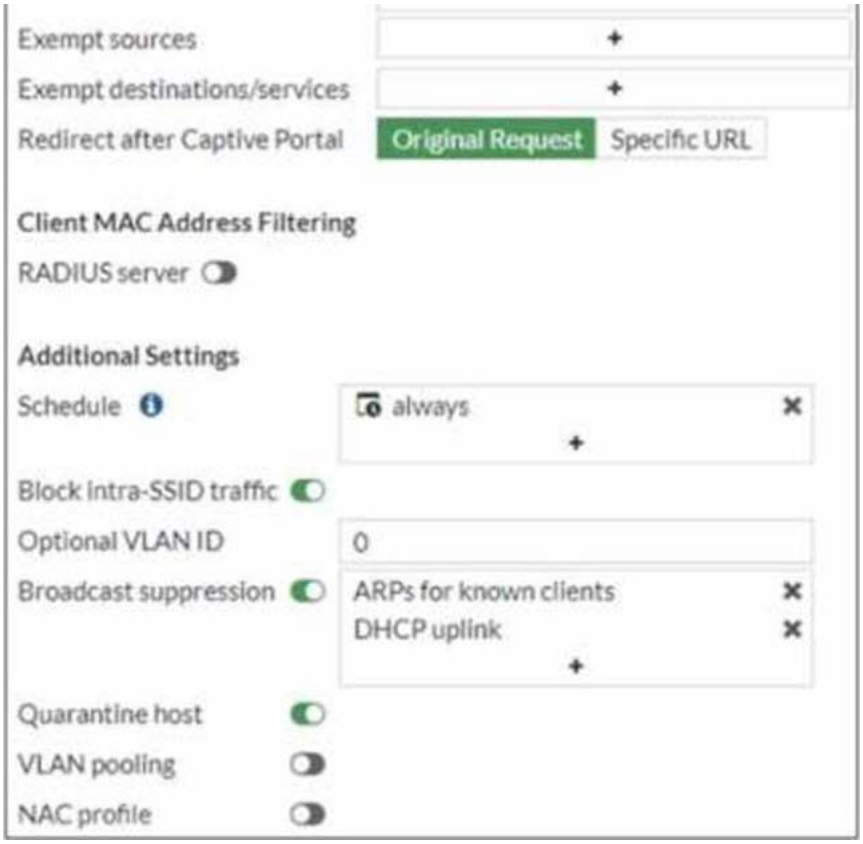
Explanation:

According to the FortiAuthenticator Administration Guide2, âWindows Active Directory domain authentication enables FortiAuthenticator to join a Windows Active Directory domain as a machine entity and proxy authentication requests using Kerberos.â Therefore, option D is true because it describes the purpose of enabling Windows Active Directory domain authentication on FortiAuthenticator. Option A is false because FortiAuthenticator does not need Windows administrator credentials to perform an LDAP lookup for a user search. Option B is false because FortiAuthenticator does not use a Windows CA certificate when authenticating RADIUS users, but

rather its own CA certificate. Option C is false because FortiAuthenticator does not import users from Windows AD, but rather synchronizes them using LDAP or FSSO.

## Question: 93

Refer to the exhibits.




Firewall Policy

```
config firewall policy
    edit 11
        set name "Guest to Internal"
        set uuid c5e45130-aada-51e8-ee0c-bc1204f9f163
        set srcintf "guest"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "FortiAuthenticator" "WindowsAD"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Examine the firewall policy configuration and SSID settings

An administrator has configured a guest wireless network on FortiGate using the external captive portal The administrator has verified that the external captive portal URL is correct However wireless

users are not able to see the captive portal login page

Given the configuration shown in the exhibit and the SSID settings which configuration change should the administrator make to fix the problem?

A. Disable the user group from the SSID configuration
B. Enable the captivs-portal-exempt option in the firewall policy with the ID 11.
C. Apply a guest.portal user group in the firewall policy with the ID 11.
D. Include the wireless client subnet range in the Exempt Source section

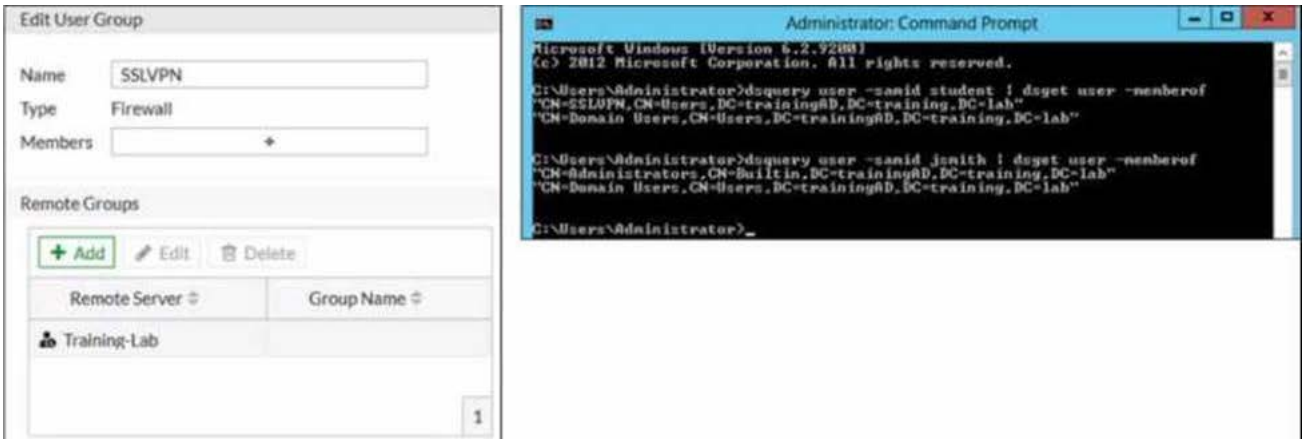
**Answer: C**

Explanation:

According to the FortiGate Administration Guide, âTo use an external captive portal, you must configure a user group that uses the external captive portal as the authentication method and apply it to a firewall policy.â Therefore, option C is true because it will allow the wireless users to be redirected to the external captive portal URL when they try to access the Internet. Option A is false because disabling the user group from the SSID configuration will prevent the wireless users from being authenticated by the FortiGate device. Option B is false because enabling the captive-portal-exempt option in the firewall policy will bypass the captive portal authentication for the wireless users, which is not the desired outcome. Option D is false because including the wireless client subnet range in the Exempt Source section will also bypass the captive portal authentication for the wireless users, which is not the desired outcome.

## Question: 94

Refer to the exhibit.




Examine the FortiGate user group configuration and the Windows AD LDAP group membership information shown in the exhibit

FortiGate is configured to authenticate SSL VPN users against Windows AD using LDAP The administrator configured the SSL VPN user group for SSL VPN users However the administrator noticed that both the student and j smith users can connect to SSL VPN

Which change can the administrator make on FortiGate to restrict the SSL VPN service to the student user only?

A. In the SSL VPN user group configuration set Group NamÂ© to CN-SSLVPN, CN="users, DC-trainingAD, DC-training, DC-lab
B. In the SSL VPN user group configuration, change Name to cn=sslvpn, CN=users, DC=trainingAD, Detraining, DC-lab.
C. In the SSL VPN user group configuration set Group Name to ::;=Domain users.CN-Users/DC=trainingAD, DC-training, DC=lab.
D. In the SSL VPN user group configuration change Type to Fortinet Single Sign-On (FSSO)

## Answer: A

Explanation:

According to the FortiGate Administration Guide, âThe Group Name is the name of the LDAP group that you want to use for authentication. The name must match exactly the name of the LDAP group on the LDAP server.â Therefore, option A is true because it will set the Group Name to match the LDAP group that contains only the student user. Option B is false because changing the Name will not affect the authentication process, as it is only a local identifier for the user group on FortiGate. Option C is false because setting the Group Name to Domain Users will include all users in the domain, not just the student user. Option D is false because changing the Type to FSSO will require a different configuration method and will not solve the problem.

## Question: 95

Refer to the exhibits.

```
# get wireless-controller rf-analysis
WTP: Office  0-192.168.5.98:5246
     channel    rssi-total    rf-score     overlap-ap    interfere-ap chan-utilizaion
           1            66           8             11              11             32%
           2            13          10              0              20             44%
           3             6          10              0              20             16%
           4            14          10              0              20             13%
           5            31          10              0              20             50%
           6           137           3              9               9             73%
           7            32          10              0              12             58%
           8            17          10              0              12              9%
           9            12          10              0              14              1%
          10            20          10              0              14             17%
          11            79           7              3               5             32%
          12            24          10              0               5             18%
          13            32          10              2               5             22%
```

Exhibit.

```
# execute ssh 192.168.5.98
admin@192.168.5.98's password:
Office # cw_diag -c all-chutil

rId=0 chan=1   2412 util=82 ( 32%)
rId=0 chan=2   2417 util=113( 44%)
rId=0 chan=3   2422 util=41 ( 16%)
rId=0 chan=4   2427 util=36 ( 14%)
rId=0 chan=5   2432 util=126( 49%)
rId=0 chan=6   2437 util=165( 73%)
rId=0 chan=7   2442 util=148( 58%)
rId=0 chan=8   2447 util=26 ( 10%)
rId=0 chan=9   2452 util=5  (  1%)
rId=0 chan=10  2457 util=46 ( 18%)
rId=0 chan=11  2462 util=82 ( 32%)
rId=0 chan=12  2467 util=45 ( 17%)
rId=0 chan=13  2472 util=50 ( 22%)
```

Examine the troubleshooting outputs shown in the exhibits

Users have been reporting issues with the speed of their wireless connection in a particular part of the wireless network The interface that is having issues is the 2 4 GHz interface that is currently configured on channel 6

The administrator of the wireless network has investigated and surveyed the local RF environment using the tools available at the AP and FortiGate

Which configuration would improve the wireless connection?

A. Change the AP 2 4 GHz channel to 11
B. Change the AP 2 4 GHz channel to 1.
C. Change the AP 2 4 GHz channel to 9.
D. Change the AP 2 4 GHz channel to 13.

**Answer: B**

Explanation:

According to the exhibits, the AP 2.4 GHz interface is currently configured on channel 6, which is overlapping with other nearby APs on channels 4 and 8. This can cause interference and reduce the wireless performance. Therefore,

changing the AP 2.4 GHz channel to 1 would improve the wireless connection, as it would avoid the overlapping channels and use a non-overlapping channel instead. Option A is false because changing the AP 2.4 GHz channel to 11 would still overlap with other nearby APs on channels 9 and 13. Option C is false because changing the AP 2.4 GHz channel to 9 would still overlap with other nearby APs on channels 6, 8, and 11. Option D is false because changing the AP 2.4 GHz channel to 13 would still overlap with other nearby APs on channels 9 and 11.

# SAMPLE QUESTIONS

*These questions are for demo purpose only.* ***Full version*** *is up to date and contains actual questions and answers.*

*Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:*

***Actual Exam Questions****: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

***Exam Dumps****: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

***Practice Tests****: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

***Guaranteed Success****: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

***Updated Content:*** *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

***Technical Support****: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*