Fortinet

NSE7_LED-7.0 Exam

Fortinet NSE 7 - LAN Edge 7.0

Questions & Answers
Demo

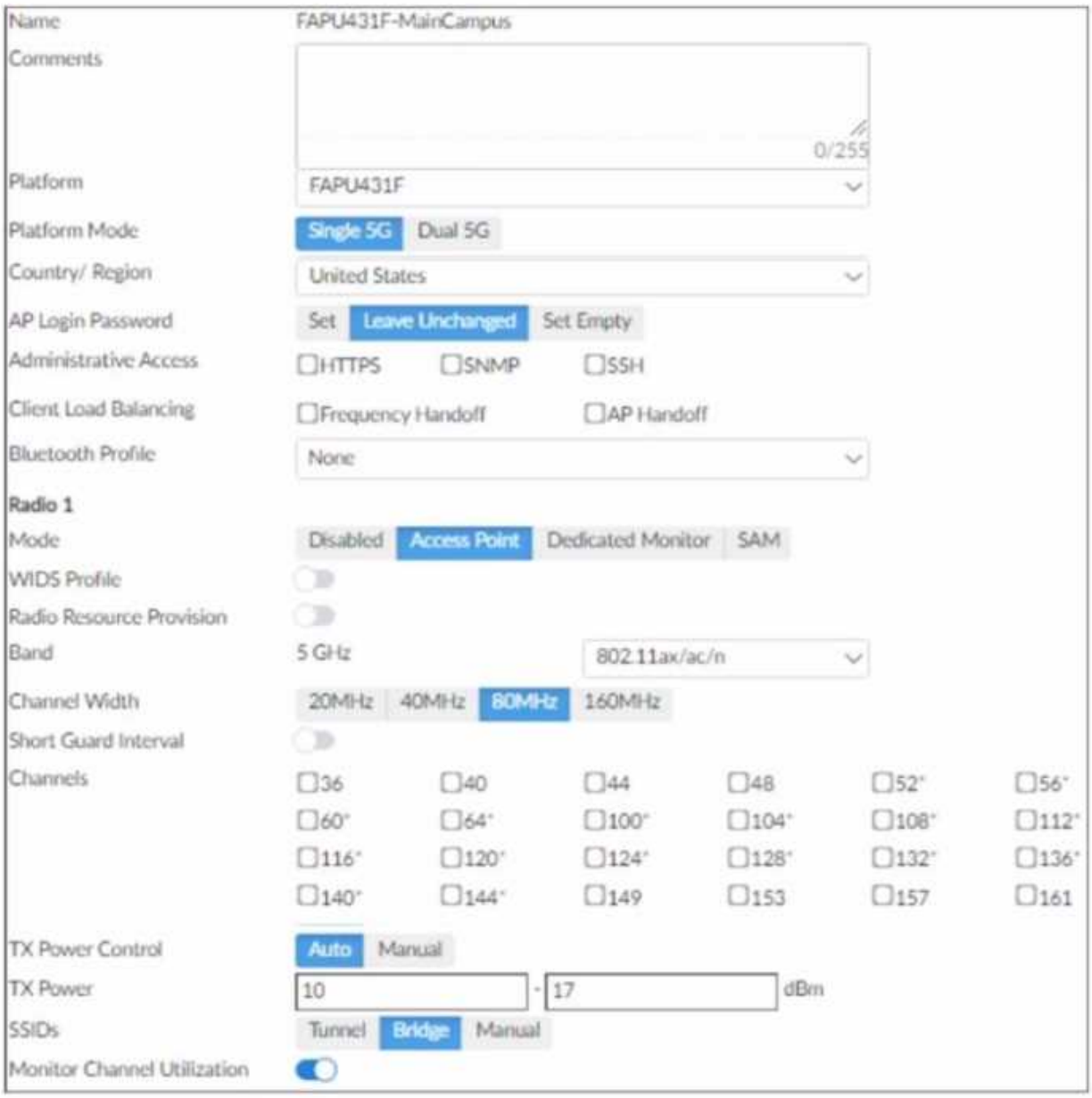
Version: 4.0

Question: 1

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

Question: 2

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: CD

Explanation:

According to the FortiAuthenticator Administration Guide2, "The 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." Therefore, option C is true. The same guide also states that "Administrators can use one or more incoming parameters to configure a mapping rule for the guest portal." 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: 3

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

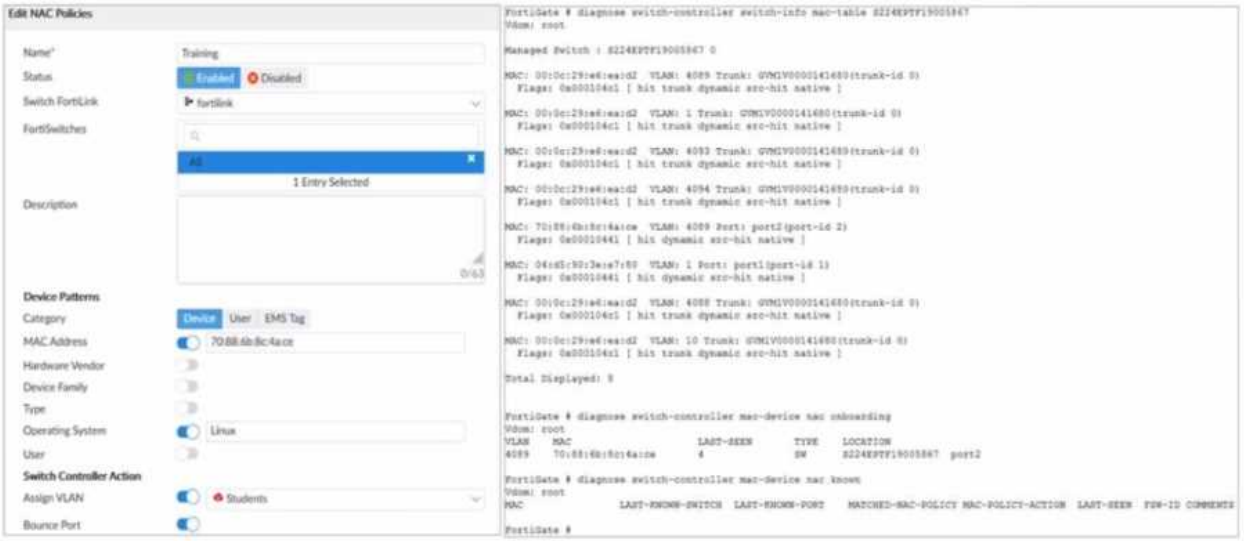
Explanation:

According to the Fortinet documentation1, “Split 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.” 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: 4

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"53€7)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

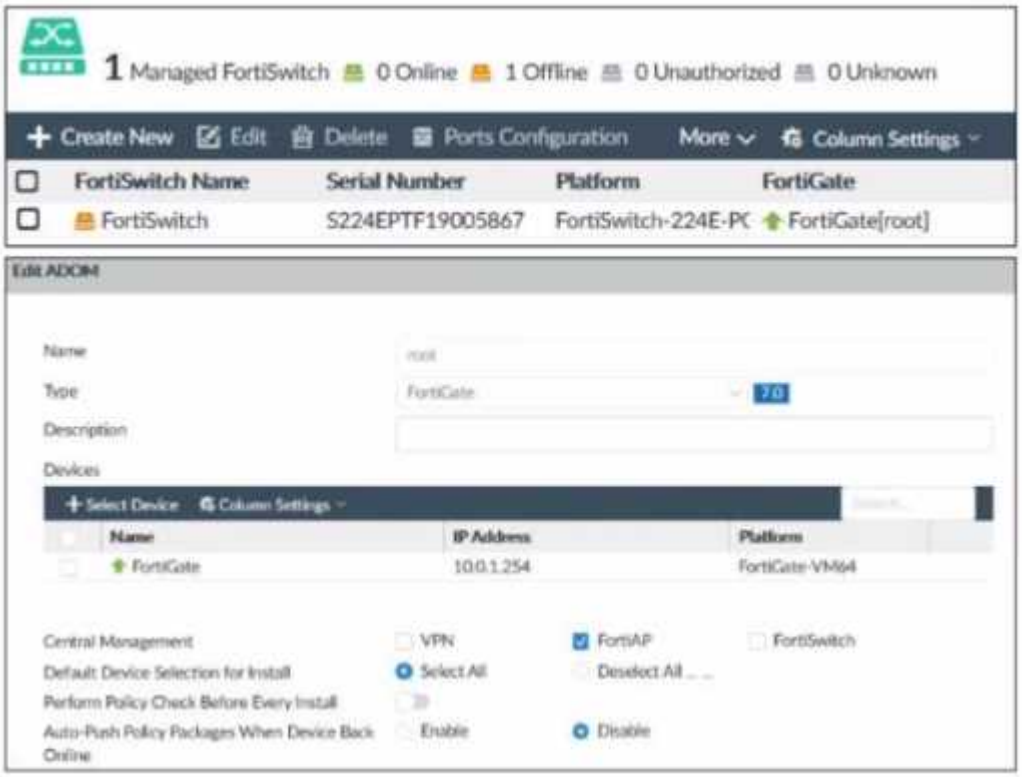
Answer: A, B

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 “config switch-controller vlan”.

Question: 5

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: CD

Explanation:

According to the FortiManager Administration Guide, “Central management mode allows you to manage all FortiSwitch devices from a single interface on the FortiManager device.” 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.

Thank You For Trying NSE7_LED-7.0 PDF Demo

To try our NSE7_LED-7.0 Premium Files visit link below:

https://examsland.com/latest-exam-questions/NSE7_LED-7.0/

Start Your NSE7_LED-7.0 Preparation