Fortinet

Exam Questions NSE7_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0

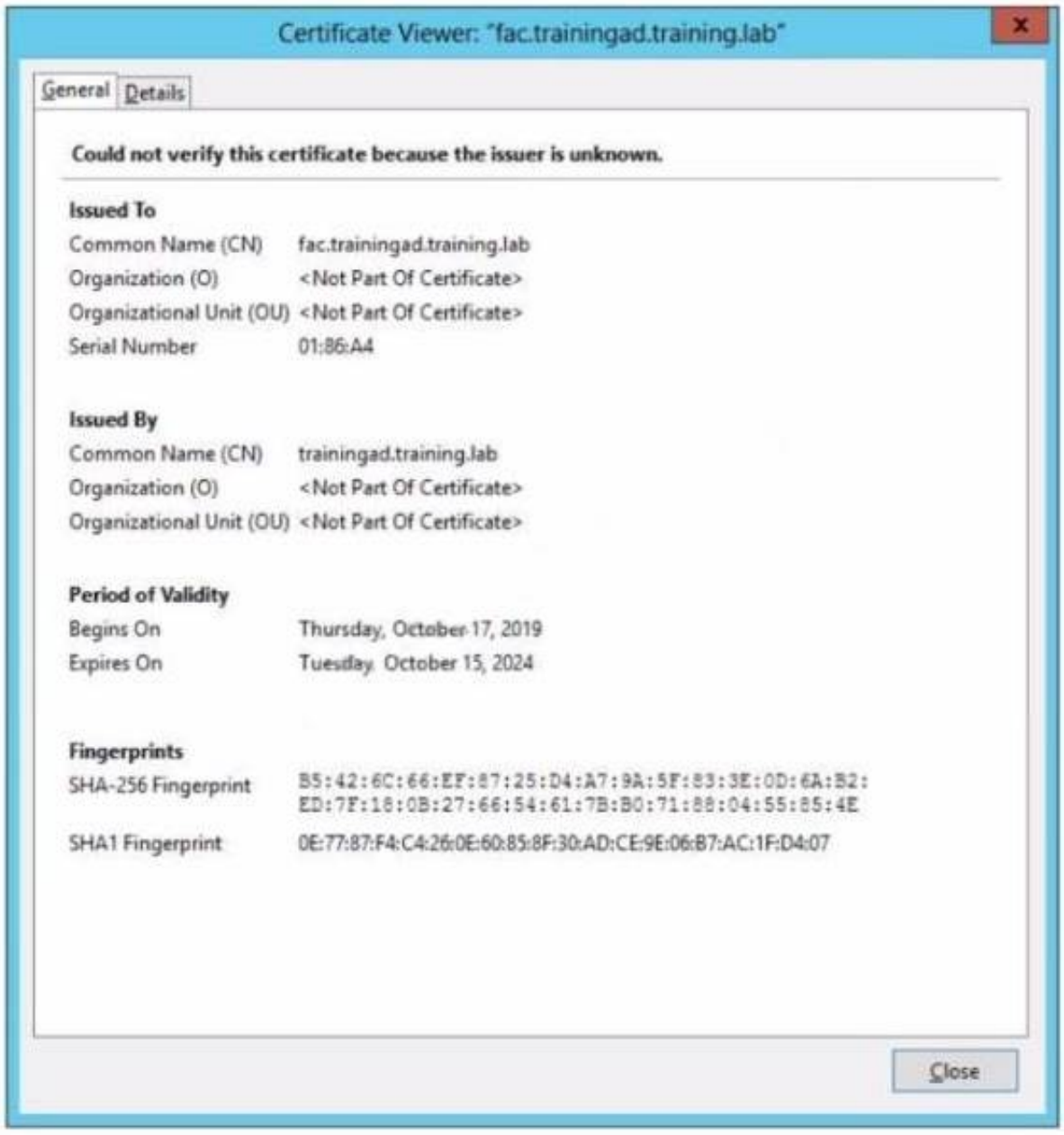
NEW QUESTION 1
Which FortiSwitch VLANs are automatically created on FortGate when the first FortiSwitch device is discovered1?

A. default quarantine, rspan voice video onboarding and nac_segment
B. access, quarantine, rspa
C. voice, video, and onboarding
D. default quarantine rspan voice video and nac_segment
E. fortilin
F. quarantine erspan voice video and onboarding

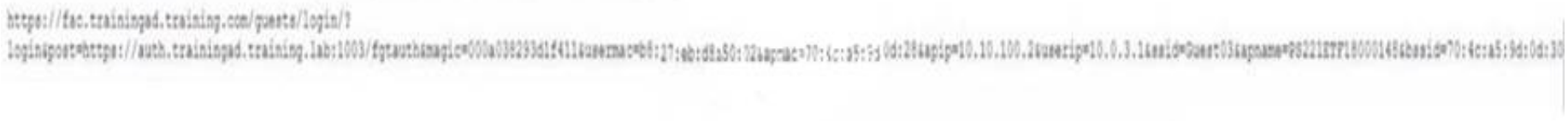
Answer: D

Explanation:
According to the FortiGate Administration Guide, “When you add a FortiSwitch device to the Security Fabric, FortiGate automatically creates the following VLANs on theFortiSwitch device: fortilink, quarantine, erspan, voice, video, and onboarding.” Therefore, option D is true because it lists the FortiSwitch VLANs that are automatically created on FortiGate when the first FortiSwitch device is discovered. Option A is false because default and nac_segment are not among the automatically created VLANs. Option B is false because access and rspan are not among the automatically created VLANs. Option C is false because default and nac_segment are not among the automatically created VLANs.

NEW QUESTION 2
Refer to the exhibit



Wireless guest users are unable to authenticate because they are getting a certificate error while loading the captive portal login page.This URL string is the HTTPS POST URL guest wireless users see when attempting to access the network using the web browser



Which two settings are the likely causes of the issue? (Choose two.)

A. The external server FQDN is incorrect
B. The wireless user's browser is missing a CA certificate
C. The FortiGate authentication interface address is using HTTPS
D. The user address is not in DDNS form

Answer: AB

Explanation:
According to the exhibit, the wireless guest users are getting a certificate error while loading the captive portal login page. This means that the browser cannot verify the identity of the server that is hosting the login page. Therefore, option A is true because the external server FQDN is incorrect, which means that it does not match the common name or subject alternative name of the server certificate. Option B is also true because the wireless user’s browser is missing a CA

certificate, which means that it does not have the root or intermediate certificate that issued the server certificate. Option C is false because the FortiGate authentication interface address is using HTTPS, which is a secure protocol that encrypts the communication between the browser and the server. Option D is false because the user address is not in DDNS form, which is not related to the certificate error.

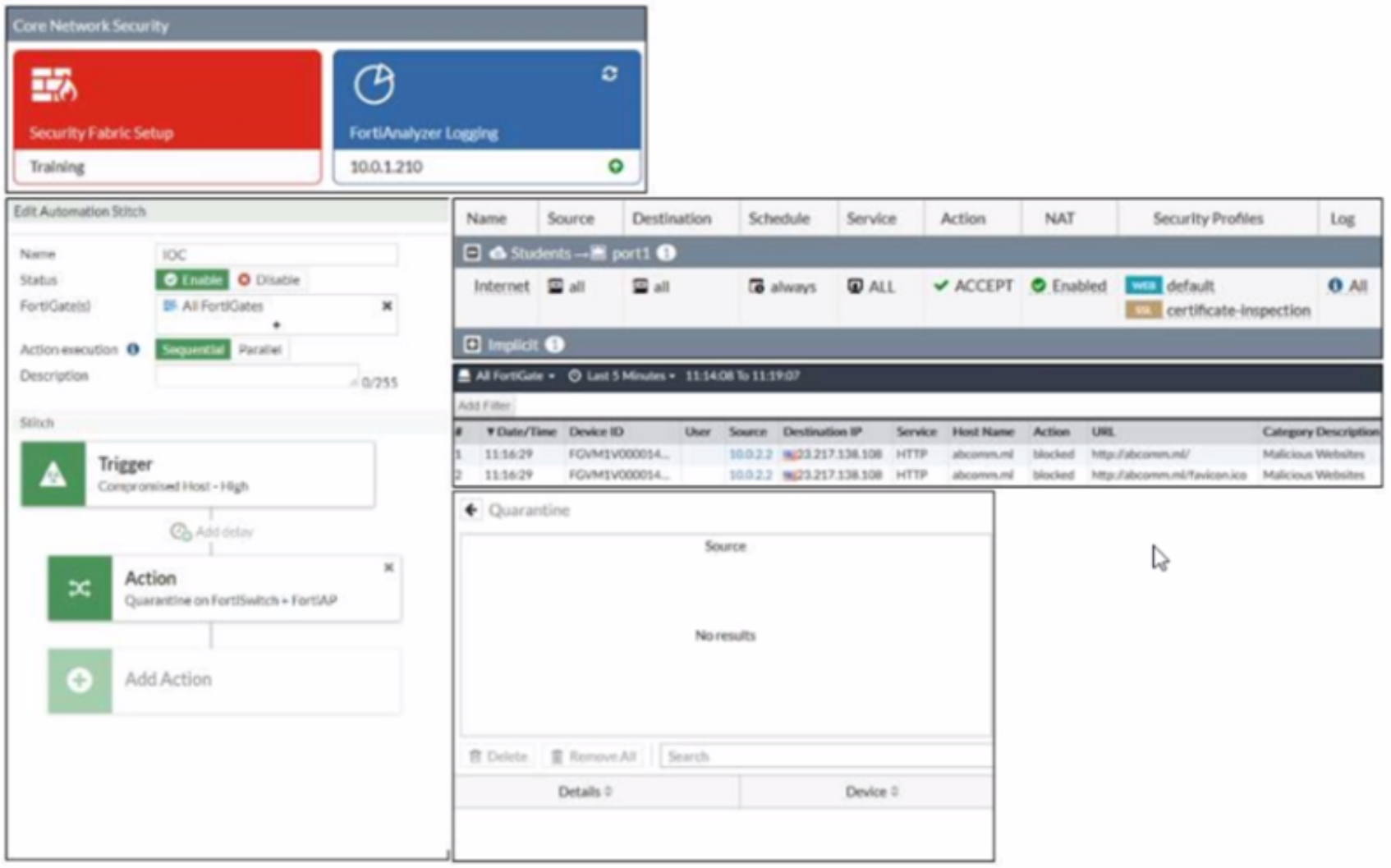
NEW QUESTION 3
Which two statements about MAC address quarantine by redirect mode are true? (Choose two)

A. The quarantined device is moved to the quarantine VLAN
B. The device MACaddress is added to the Quarantined Devices firewall address group
C. It is the default mode for MAC address quarantine
D. The quarantined device is kept in the current VLAN

Answer: BD

Explanation:
According to the FortiGate Administration Guide, “MAC address quarantine by redirect mode allows you to quarantine devices by adding their MAC addresses to a firewall address group called Quarantined Devices. The quarantined devices are kept in their current VLANs, but their traffic is redirected to a quarantine portal.” Therefore, options B and D are true because they describe the statements about MAC address quarantine by redirect mode. Option A is false because the quarantined device is not moved to the quarantine VLAN, but rather kept in the current VLAN. Option C is false because redirect mode is not the default mode for MAC address quarantine, but rather an alternative mode that can be enabled by setting mac-quarantine-mode to redirect.
https://docs.fortinet.com/document/fortiap/7.0.0/configuration-guide/734537/radius-authenticated-dynamic-vlan
: https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/734537/mac-address-quarantine

NEW QUESTION 4
Refer to the exhibit.



Examine the FortiGate configuration FortiAnalyzer logs and FortiGate widget shown in the exhibit
An administrator is testing the Security Fabric quarantine automation The administrator added FortiAnalyzer to the Security Fabric and configured an automation stitch to automatically quarantine compromised devices The test device (::.:.:.!) s connected to a managed Fort Switch dev :e
After trying to access a malicious website from the test device, the administrator verifies that FortiAnalyzer has a log (or the test connection However the device is not getting quarantined by FortiGate as shown in the quarantine widget
Which two scenarios are likely to cause this issue? (Choose two)

A. The web filtering rating service is not working
B. FortiAnalyzer does not have a valid threat detection services license
C. The device does not have FortiClient installed
D. FortiAnalyzer does not consider the malicious website an indicator of compromise (IOC)

Answer: BD

Explanation:
According to the exhibits, the administrator has configured an automation stitch to automatically quarantine compromised devices based on FortiAnalyzer’s threat detection services. However, according to the FortiAnalyzer logs, the test device is not detected as compromised by FortiAnalyzer, even though it tried to access a malicious website. Therefore, option B is true because FortiAnalyzer does not have a valid threat detection services license, which is required to enable the threat detection services feature. Option D is also true because FortiAnalyzer does not consider the malicious website an indicator of compromise (IOC), which is a criterion for identifying compromised devices. Option A is false because the web filtering rating service is working, as shown by the log entry that indicates that the test device accessed a URL with a category of “Malicious Websites”. Option C is false because the device does not need to have FortiClient installed to be quarantined by FortiGate, as long as it is connected to a managed FortiSwitch device.

NEW QUESTION 5
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.

NEW QUESTION 6
Which two statements about FortiSwitchmanager are true1? (Choose two)

A. Per-device management is the default management mode on FortiManager
B. FortiManager obtains the FortiSwitch status information by querying the FortiGate REST API every three minutes
C. If the administrator makes any changes on FortiSwitch manager they must also install those changes on FortiGate so that those changes are applied on the managed switches
D. Any switch discovered or authorized on FortiGate must be added manually on FortiSwitch manager

Answer: BC

Explanation:
According to the FortiManager Administration Guide1, “FortiManager obtains the FortiSwitch status information by querying the FortiGate REST API every three minutes.” Therefore, option B is true because it describes how FortiManager gets the information about the managed switches. According to the same guide2, “If you make any changes in this module, you must install them on your managed device so that they are applied on your managed switches.” Therefore, option C is true because it describes what the administrator must do after making any changes on FortiSwitch manager. Option A is false because central management is the default management mode on FortiManager, not per-device management. Option D is false because anyswitch discovered or authorized on FortiGate will be automatically added on FortiSwitch manager, not manually.
1: https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/734537/fortiswitch-manager 2: https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/734537/fortiswitch-manager#fortisw

NEW QUESTION 7
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

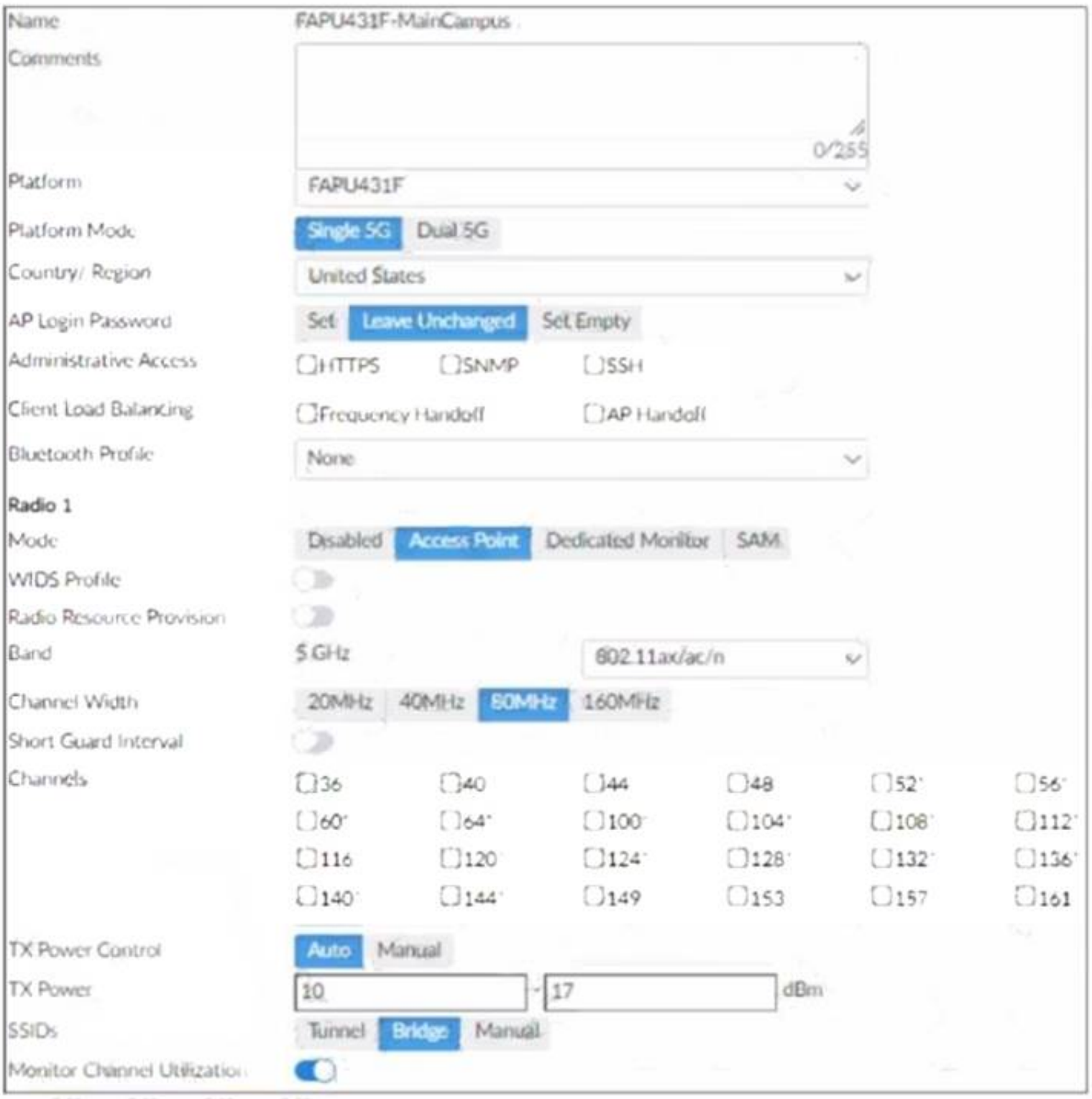
Answer: A

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.

NEW QUESTION 8
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.

NEW QUESTION 9
Refer to the exhibit

```
config vpn certificate ocsp-server
    edit "FAC"
        set url "http://10.0.1.150:2560"
        set cert "CA_Cert_1"
        set unavail-action revoke
    next
end
config vpn certificate setting
    set ocsp-status enable
    set ocsp-option server
    set ocsp-default-server "FAC"
    set strict-ocsp-check enable
end
config user peer
    edit "student"
        set ca "CA_Cert_1"
    next
end
```

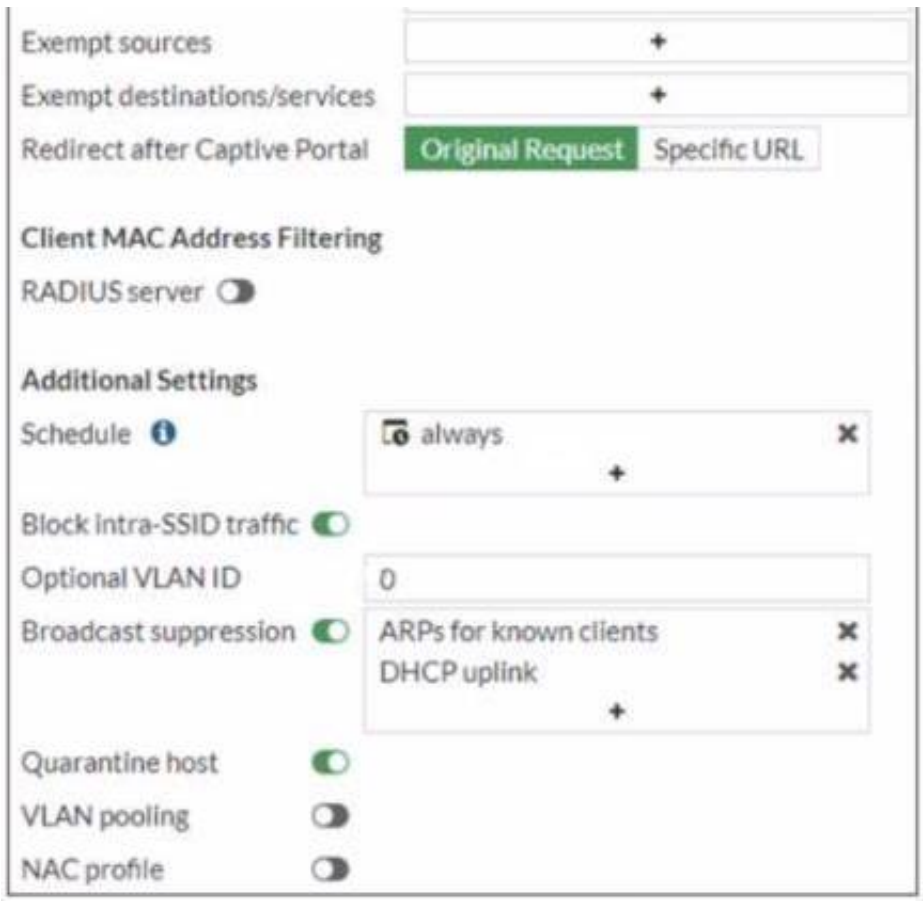
Examine the sections of the configuration shown in the output
What action will FortiGate take when verifying the student certificate through OCSP?

A. Reject the student certificate if the OCSP server replies that the student certificate status is unknown
B. Not verify the OCSP server certificate
C. Use the OCSP URL included in the student certificate to verify the student certificate
D. Consider the student certificate status as valid if the OCSP server is unreachable

Answer: C

Explanation:
According to the exhibit, the FortiGate configuration has ocsp-status enabled and ocsp-option set to certificate.
This means that FortiGate will use OCSP to verify the revocation status of certificates presented by
clients. According to the FortiGate Administration Guide2, “If you select certificate, FortiGate uses an OCSP URL included in a certificate to verify that certificate.”
Therefore, option C is true because it describes what action FortiGate will take when verifying the student certificate through OCSP. Option A is false because FortiGate will not reject the student certificate if the OCSP server replies that the student certificate status is unknown, but rather accept it as valid. Option B is false because FortiGate will verify the OCSPserver certificate by default, unless strict-ocsp-check is disabled. Option D is false because FortiGate will not consider the student certificate status as valid if the OCSP server is unreachable, but rather reject it as invalid.

NEW QUESTION 10
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, “To 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.” 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.

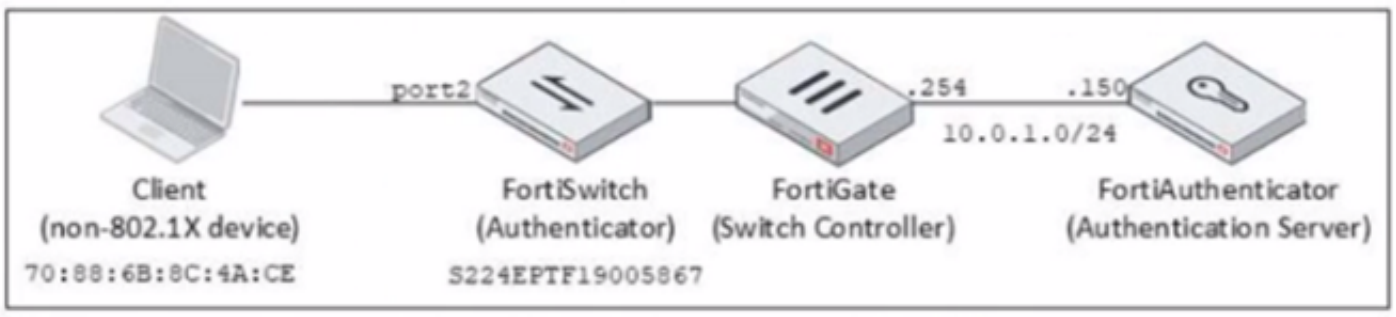
NEW QUESTION 10
When you configure a FortiAP wireless interface for auto TX power control which statement describes how it configures its transmission power"?

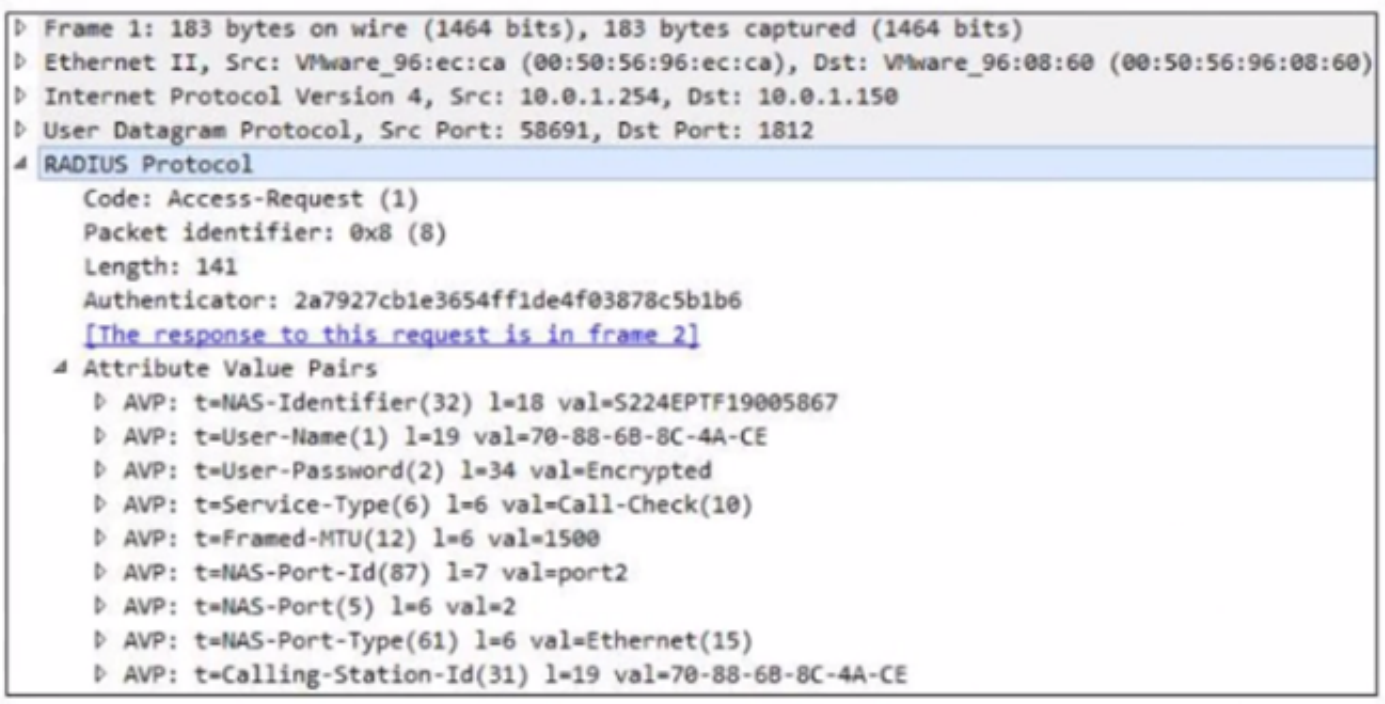
A. Every 30 seconds the AP will measure the signal strength of the AP using the client The AP will adjust its signal strength up or down until the AP signal is detected at -70 dBm
B. Every 30 seconds FortiGate measures the signal strength of adjacent AP interfaces It will adjust its own AP power to match the adjacent AP signal strength
C. Every 30 seconds FortiGate measures the signal strength of adjacent FortiAP interfaces It will adjust the adjacent AP power to be detectable at -70 dBm
D. Every 30 seconds FortiGate measures the signal strength of the weakest associated client The AP will then configure its radio power to match the detected signal strength of the client

Answer: A

Explanation:
According to the FortiAP Configuration Guide1, “Auto TX power control allows the AP to adjust its transmit power based on the signal strength of the client. The AP will measure the signal strength of the client every 30 seconds and adjust its transmit power up or down until the client signal is detected at -70 dBm.” Therefore, option A is true because it describes how the FortiAP wireless interface configures its transmission power when auto TX power control is enabled. Option B is false because FortiGate does not measure the signal strength of adjacent AP interfaces, but rather the FortiAP does. Option C is false because FortiGate does not
adjust the adjacent AP power, but rather the FortiAP adjusts its own power. Option D is false becauseFortiGate does not measure the signal strength of the weakest associated client, but rather the FortiAP does.

NEW QUESTION 11
Refer to the exhibit.





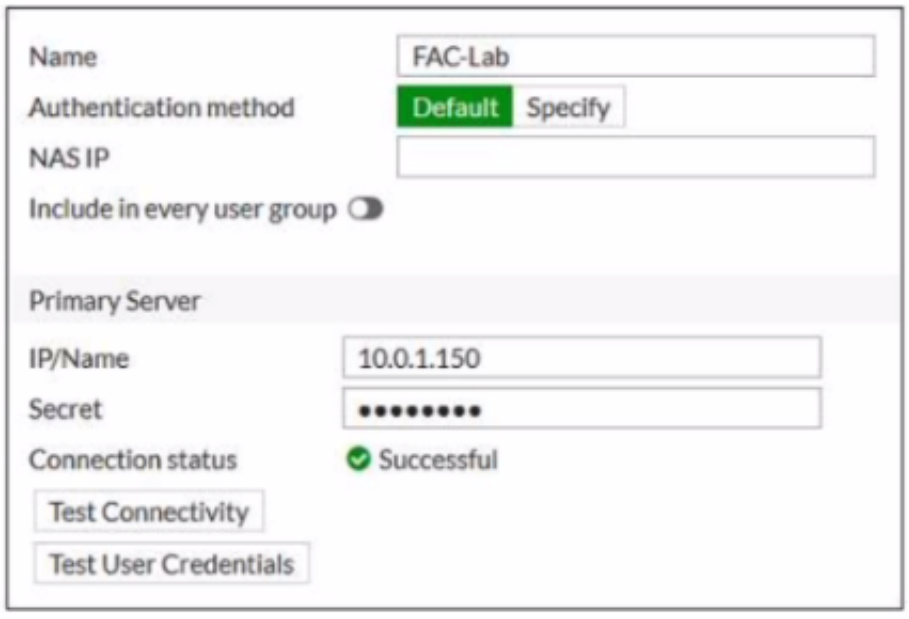
Examine the network diagram and packet capture shown in the exhibit
The packet capture was taken between FortiGate and FortiAuthenticator and shows a RADIUS Access-Request packet sent by FortiSwitch to FortiAuthenticator through FortiGate
Why does the User-Name attribute in the RADIUS Access-Request packet contain the client MAC address?

A. The client is performing AD machine authentication
B. FortiSwitch is authenticating the client using MAC authentication bypass
C. The client is performing user authentication
D. FortiSwitch is sending a RADIUS accounting message to FortiAuthenticator

Answer: B

Explanation:
According to the exhibit, the User-Name attribute in the RADIUS Access-Request packet contains the client MAC address of 00:0c:29:6a:2b:3d. This indicates that FortiSwitch is authenticating the client using MAC authentication bypass (MAB), which is a method of authenticating devices that do not support 802.1X by using their MAC address as the username and password. Therefore, option B is true because it explains why the User-Name attribute contains the client MAC address. Option A is false because AD machine authentication uses a computer account name and password, not a MAC address. Option C is false because user authentication uses a user name and password, not a MAC address. Option D is false because FortiSwitch is sending a RADIUS Access-Request message to FortiAuthenticator, not a RADIUS accounting message.

NEW QUESTION 16
Refer to the exhibit.



Examine the RADIUS server configuration shown in the exhibit
An administrator has configured a RADIUS server on FortiGate that points to FortiAuthenticator FortiAuthenticator is acting as an authentication proxy and is configured to relay all authentication requests to a remote Windows AD server using LDAP
While testing the configuration the administrator noticed that the diagnosetest authserver command worked with PAP, however authentication requests failed when using MSCHAP2
Which two solutions can the administrator implement to get MSCHAP2 authentication to work" (Choose two.)

A. On FortiAuthenticator enable Windows Active Directory Domain Authentication to add FortiAuthenticator to the Windows domain
B. On FortiGate configure the NAS IP setting on the RADIUS server
C. On FortiAuthenticator change the back-end authentication server from LDAP to RADIUS
D. On FortiGate update the Secret setting on the RADIUS server

Answer: AC

Explanation:
According to the exhibit, the RADIUS server configuration on FortiGate points to FortiAuthenticator, which is acting as an authentication proxy and is configured to relay all authentication requests to a remote Windows AD server using LDAP. However, LDAP does not support MSCHAP2 authentication, which is required for RADIUS. Therefore, option A is true because on FortiAuthenticator, enabling Windows Active Directory Domain Authentication will add FortiAuthenticator to the Windows domain and allow it to use MSCHAP2 authentication with the AD server. Option C is also true because on FortiAuthenticator, changing the back-end authentication server from LDAP to RADIUS will allow it to use MSCHAP2 authentication with the AD server. Option B is false because on FortiGate, configuring the NAS IP setting on the RADIUS server will not affect the MSCHAP2 authentication, but rather the source IP address of the RADIUS packets. Option D is false because on FortiGate, updating the Secret setting on the RADIUS server will not affect the MSCHAP2 authentication, but rather the shared secret between FortiGate and FortiAuthenticator.

NEW QUESTION 19
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.

NEW QUESTION 23
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE7_LED-7.0 Practice Exam Features:

* NSE7_LED-7.0 Questions and Answers Updated Frequently

* NSE7_LED-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_LED-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_LED-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year