# Fortinet

## Exam Questions NSE7_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0

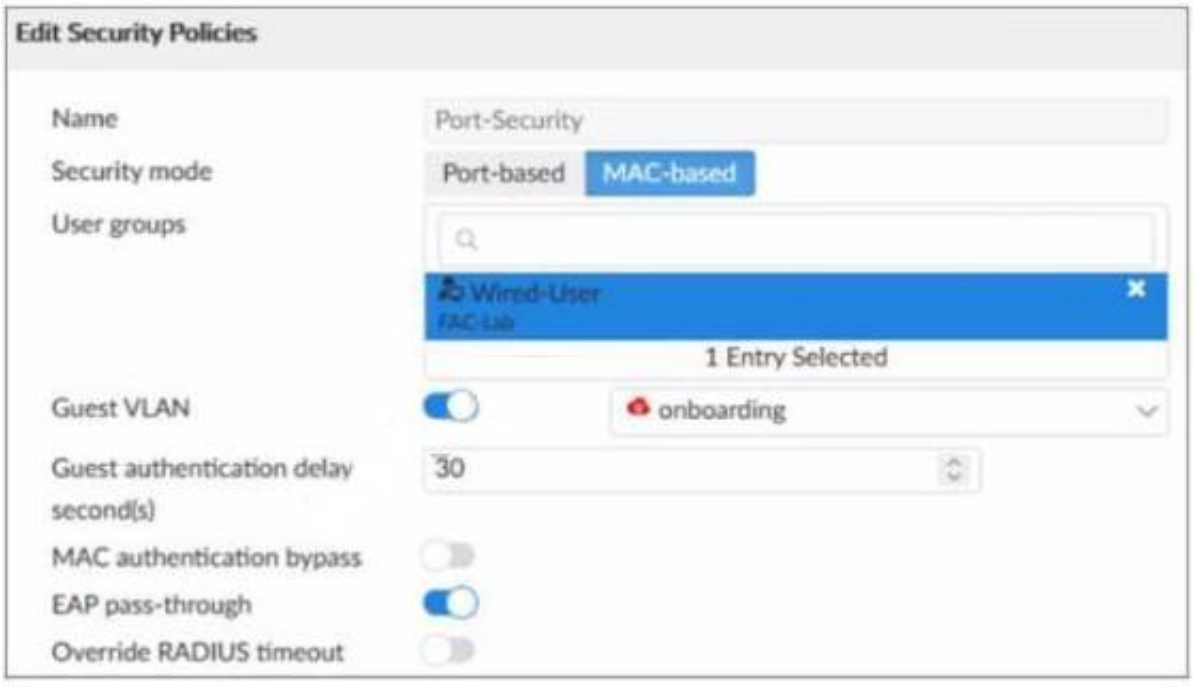
**NEW QUESTION 1**
Which FortiSwitch VLANs are automatically created on FortGate when the first FortiSwitch device is discovered1?

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.



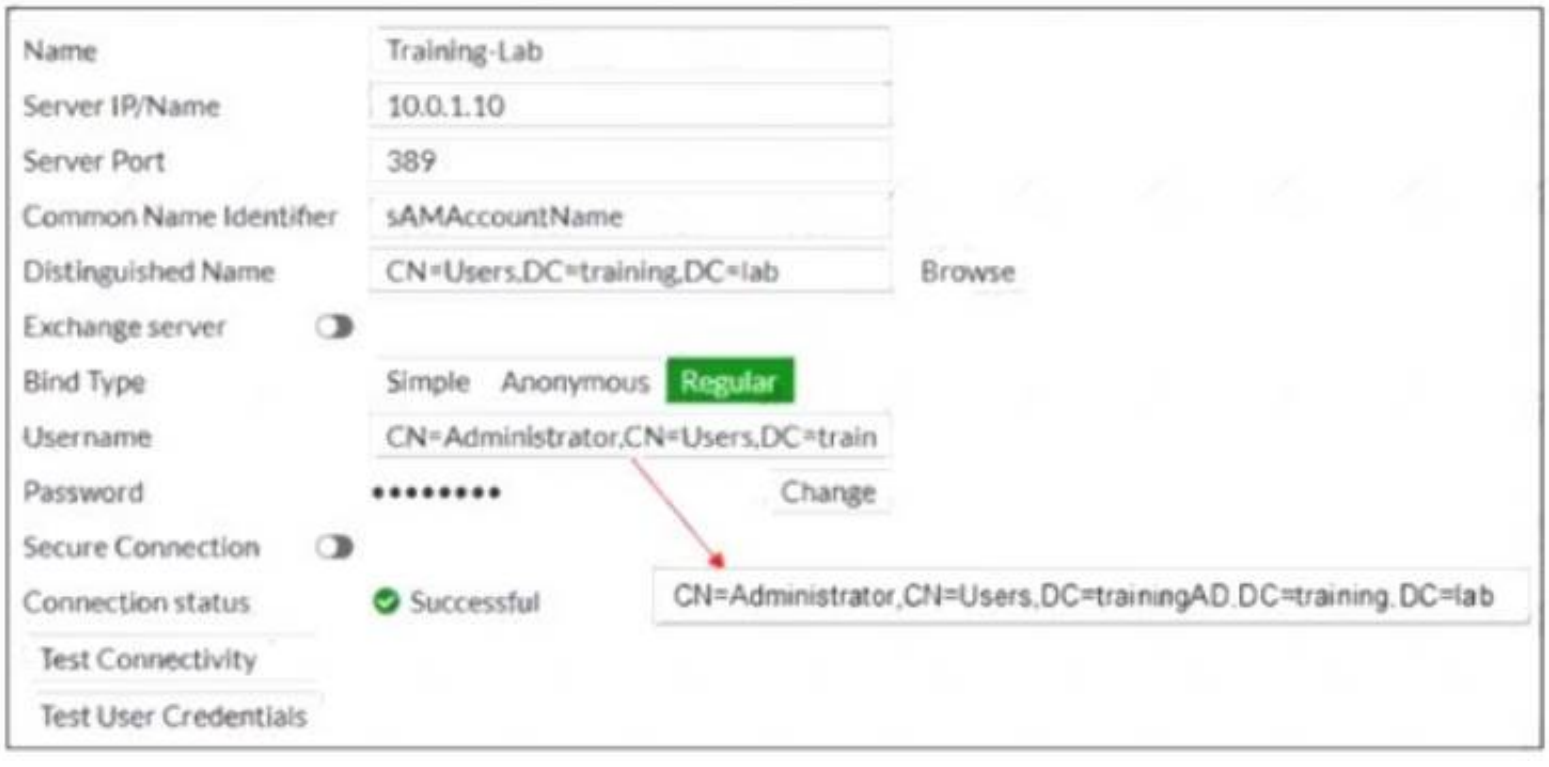

Examine the FortiSwitch security policy shown in the exhibit
If the security profile shown in the exhibit is assigned to all ports on a FortiSwitch device for 802 1X authentication which statement about the switch is correct?

A. FortiSwitch cannot authenticate multiple devices connected to the same port
B. FortiSwitch will try to authenticate non-802 1X devices using the device MAC address as the username and password
C. FortiSwitch will assign non-802 1X devices to the onboarding VLAN
D. All EAP messages will be terminated on FortiSwitch

**Answer:** C

**Explanation:**
According to the FortiSwitch Administration Guide, “If a device does not support 802.1X authentication, you can configure the switch to assign the device to an onboarding VLAN. The onboarding VLAN is a separate VLAN that you can use to provide limited network access to non-802.1X devices.” Therefore, option C is true because it describes the behavior of FortiSwitch when the security profile shown in the exhibit is assigned to all ports. Option A is false because FortiSwitch can authenticate multiple devices connected to the same port using MAC-based or MAB-EAP modes. Option B is false because FortiSwitch will not try to authenticate non-802.1X devices using the device MAC address as the username and password, but rather use MAC authentication bypass (MAB) or EAP pass-through modes. Option D is false because all EAP messages will be terminated on FortiGate, not FortiSwitch, when using 802.1X authentication.

**NEW QUESTION 3**
Refer to the exhibit.




Examine the LDAP server configuration shown in the exhibit Note that the Username setting has been expanded to display Its full content
On the Windows AD server 10.0.1.10, the administrator used dsquery. which returned the following output:

```
>dsquery user -samid student
"CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab"
```

According to the output which FortiGate LDAP setting is configured incorrectly"

A. Common Name Identifier
B. Bind Type
C. Distinguished Name
D. Username

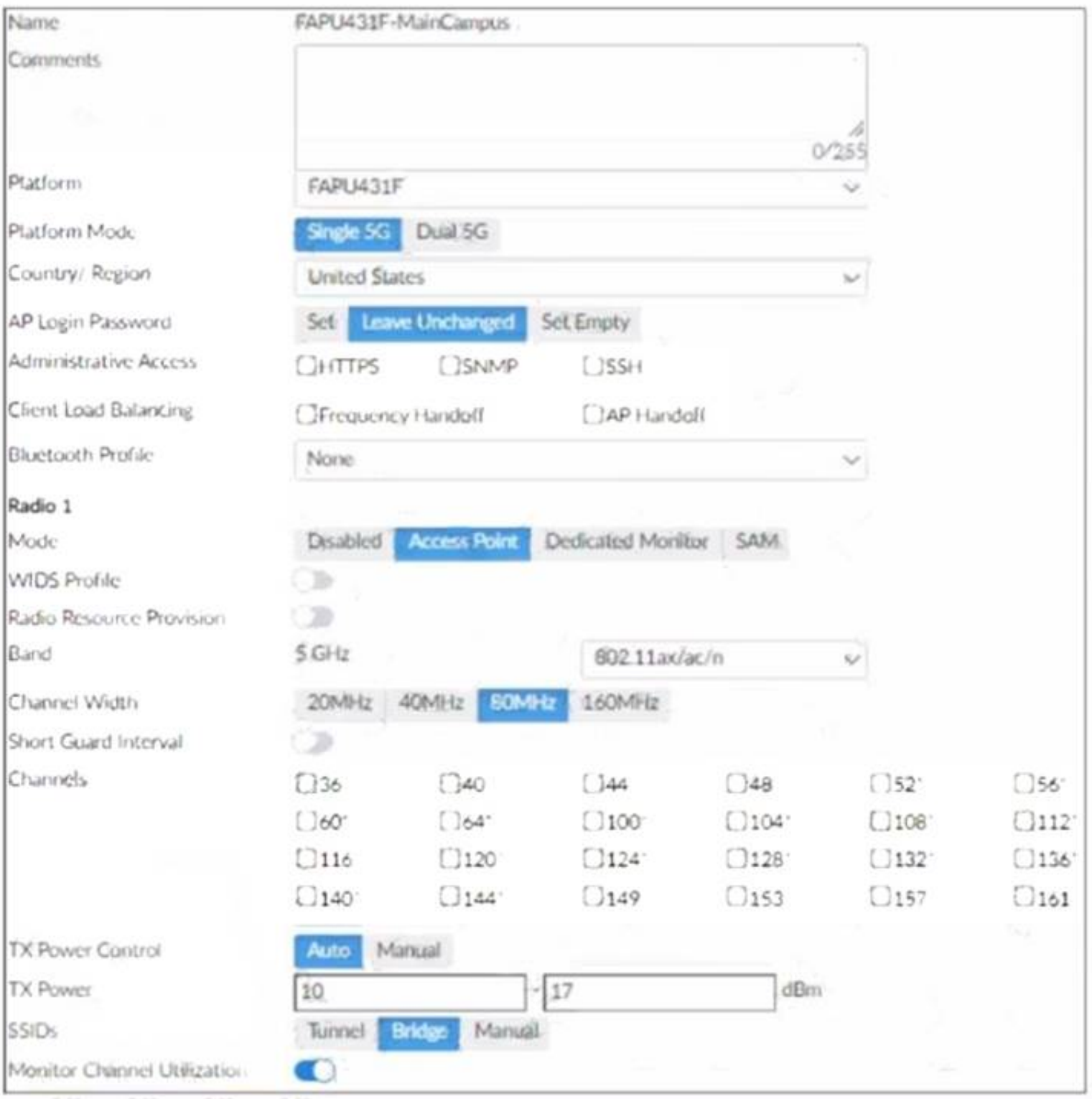
**Answer:** C

**Explanation:**
According to the exhibits, the LDAP server configuration on FortiGate has the Distinguished Name set to “dc=training,dc=lab”. However, according to the output of the dsquery command on the Windows AD server, the Distinguished Name of the domain should be “dc=trainingAD,dc=training,dc=lab”. Therefore, option C is true because the Distinguished Name on FortiGate is configured incorrectly and does not match the actual Distinguished Name of the domain. Option A is false because the Common Name Identifier on FortiGate is configured correctly as “cn”. Option B is false because the Bind Type on FortiGate is configured correctly as “Regular”. Option D is false because the Username on FortiGate is configured correctly as “cn=admin,cn=users,dc=trainingAD,dc=training,dc=lab”.

**NEW QUESTION 4**
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 5**
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:** AC

**Explanation:**
According to the FortiAP Configuration 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. You must also enable Broadcast SSID.” 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, “You can create AP groups and assign them to different locations or departments. You can then apply different settings, such as SSIDs, to each group.” 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.

**NEW QUESTION 6**
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 7**
Refer to the exhibit.

```
config system dhcp server
    edit 1
        set ntp-service local
        set default-gateway 169.254.1.1
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 169.254.1.2
                set end-ip 169.254.1.254
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch" "FortiExtende
    next
end
```

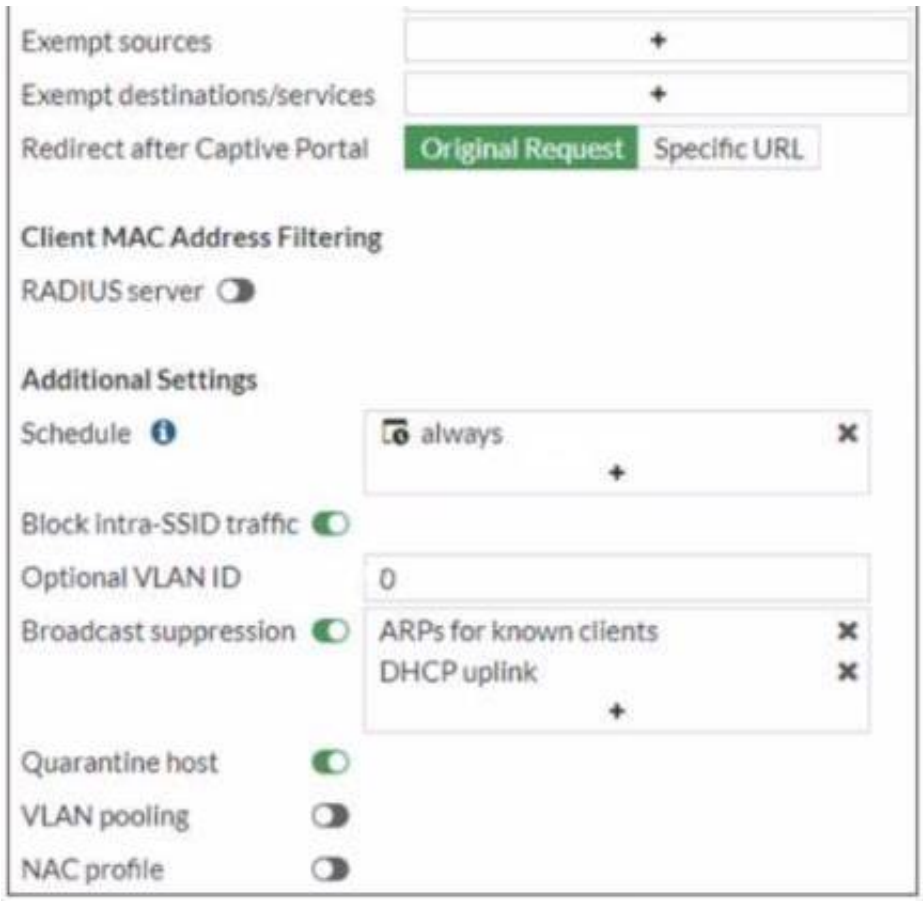
By default FortiOS creates the following DHCP server scope for the FortiLink interface as shown in the exhibit
What is the objective of the vci-string setting?

A. To ignore DHCP requests coming from FortiSwitch and FortiExtender devices
B. To reserve IP addresses for FortiSwitch and FortiExtender devices
C. To restrict the IP address assignment to FortiSwitch and FortiExtender devices
D. To restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname

**Answer:** C

**Explanation:**
According to the exhibit, the DHCP server scope for the FortiLink interface has a vci-string setting with the value “Cisco AP c2700”. This setting is used to match the vendor class identifier (VCI) of the DHCP clients that request an IP address from the DHCP server. The VCI is a text string that uniquely identifies a type of vendor device. Therefore, option C is true because the vci-string setting restricts the IP address assignment to FortiSwitch and FortiExtender devices, which use the VCI “Cisco AP c2700”. Option A is false because the vci-string setting does not ignore DHCP requests coming from FortiSwitch and FortiExtender devices, but rather accepts them. Option B is false because the vci-string setting does not reserve IP addresses for FortiSwitch and FortiExtender devices, but rather assigns them dynamically. Option D is false because the vci-string setting does not restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname, but rather to devices that have “Cisco AP c2700” as their VCI.

**NEW QUESTION 8**
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 9**
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 10**
Which EAP method requires the use of a digital certificate on both the server end and the client end?

A. EAP-TTLS
B. PEAP
C. EAP-GTC
D. EAP-TLS

**Answer:** D

**Explanation:**
According to the FortiGate Administration Guide, “EAP-TLS is the most secure EAP method. It requires a digital certificate on both the server end and the client end. The server and client authenticate each other using
their certificates.” Therefore, option D is true because it describes the EAP method that requires the use of a digital certificate on both the server end and the client end. Option A is false because EAP-TTLS only requires a digital certificate on the server end, not the client end. Option B is false because PEAP also only requires a digital certificate on the server end, not the client end. Option C is false because EAP-GTC does not require a digital certificate on either the server end or the client end.

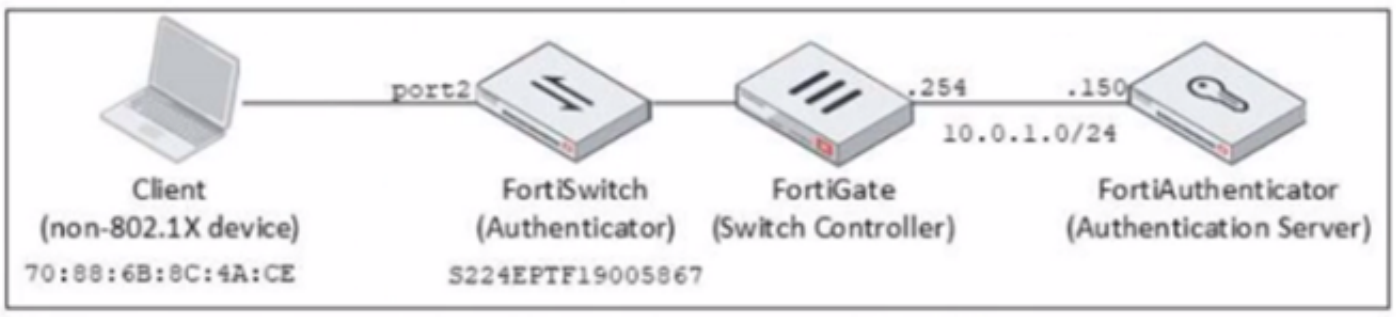
**NEW QUESTION 10**
Which CLI command should an administrator use to view the certificate verification process in real time?

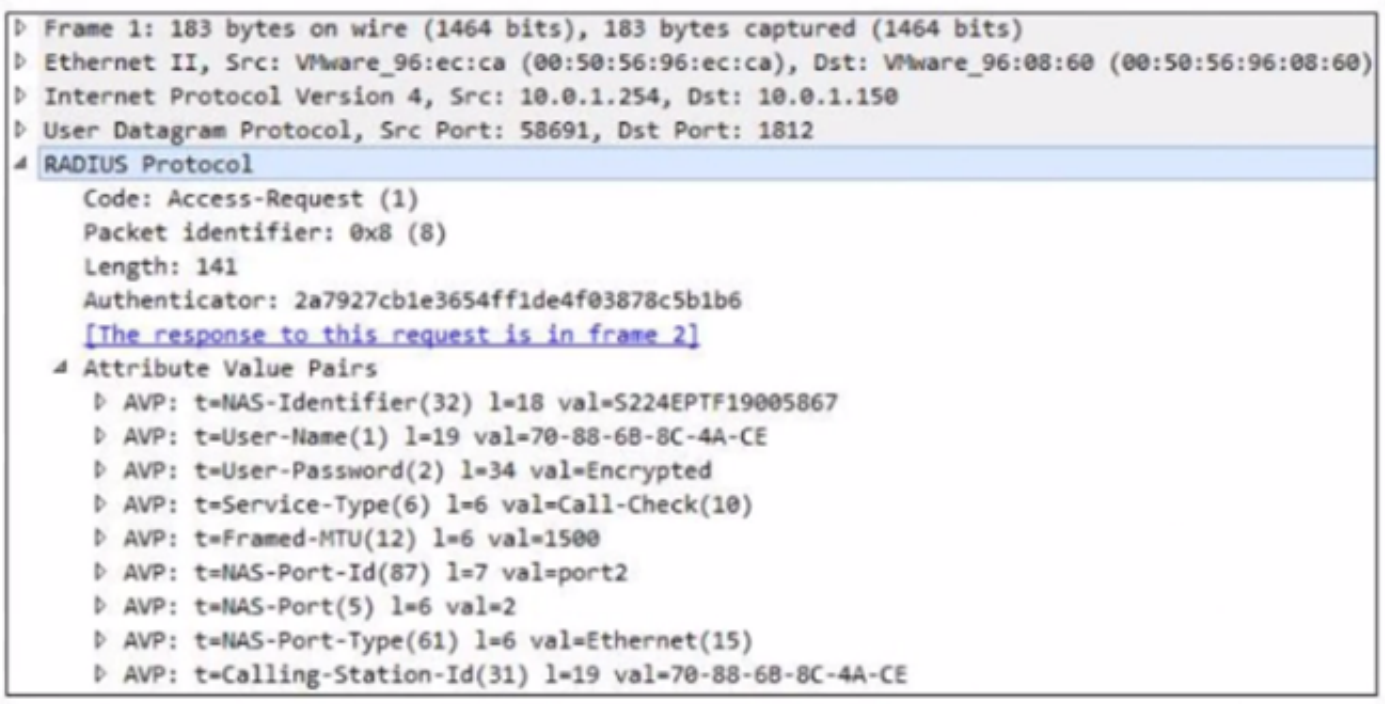
A. diagnose debug application foauthd -1
B. diagnose debug application radiusd -1
C. diagnose debug application authd -1
D. diagnose debug application fnbamd -1

**Answer:** A

**Explanation:**
According to the FortiOS CLI Reference Guide, “The diagnose debug application foauthd command enables debugging of certificate verification process in real time.” Therefore, option A is true because it describes the CLI command that an administrator should use to view the certificate verification process in real time. Option B is false because diagnose debug application radiusd -1 enables debugging of RADIUS authentication process, not certificate verification process. Option C is false because diagnose debug application authd -1 enables debugging of authentication daemon process, not certificate verification process. Option D is false because diagnose debug application fnbamd -1 enables debugging of FSSO daemon process, not certificate verification process.

**NEW QUESTION 11**
Refer to the exhibit.



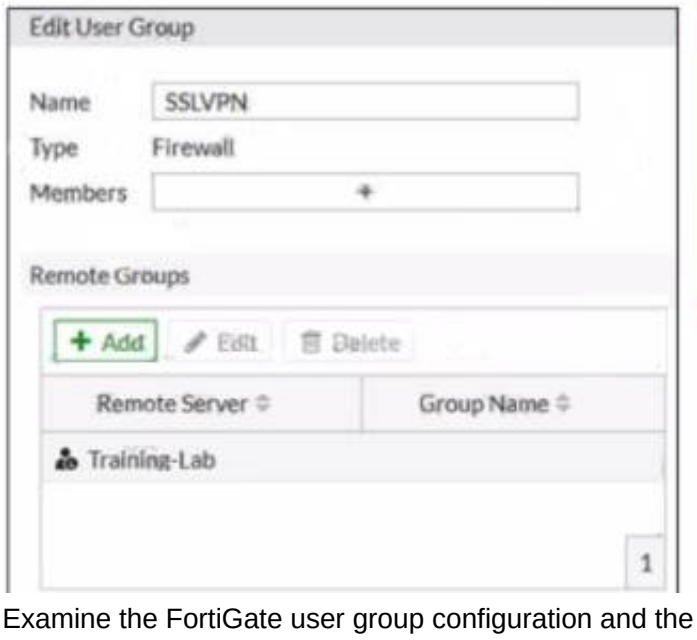

Examine the network diagram and packet capture shown in the exhibit
The packet capture was taken between FortiGate and FortiAuthenticator and shows a RADIUS Access-Request packet sent by FortiSwitch to FortiAuthenticator through FortiGate
Why does the User-Name attribute in the RADIUS Access-Request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

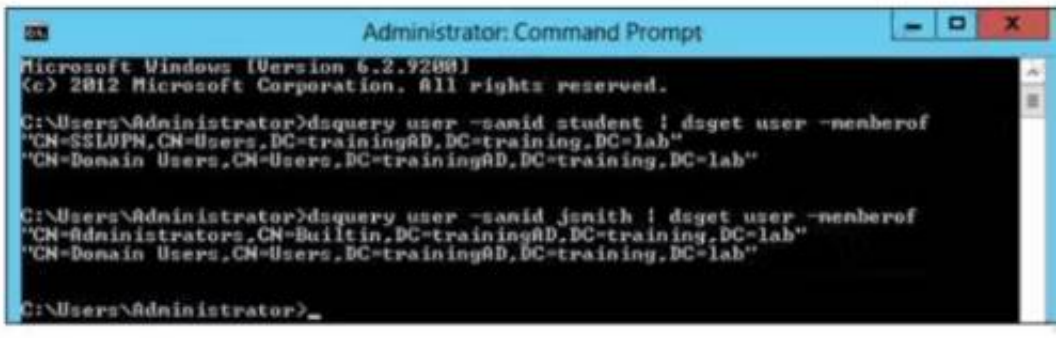
A. The client is performing AD machine authentication
B. FortiSwitch is authenticating the client using MAC authentication bypass
C. The client is performing user authentication
D. FortiSwitch is sending a RADIUS accounting message to FortiAuthenticator

**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 14**
Refer to the exhibit.



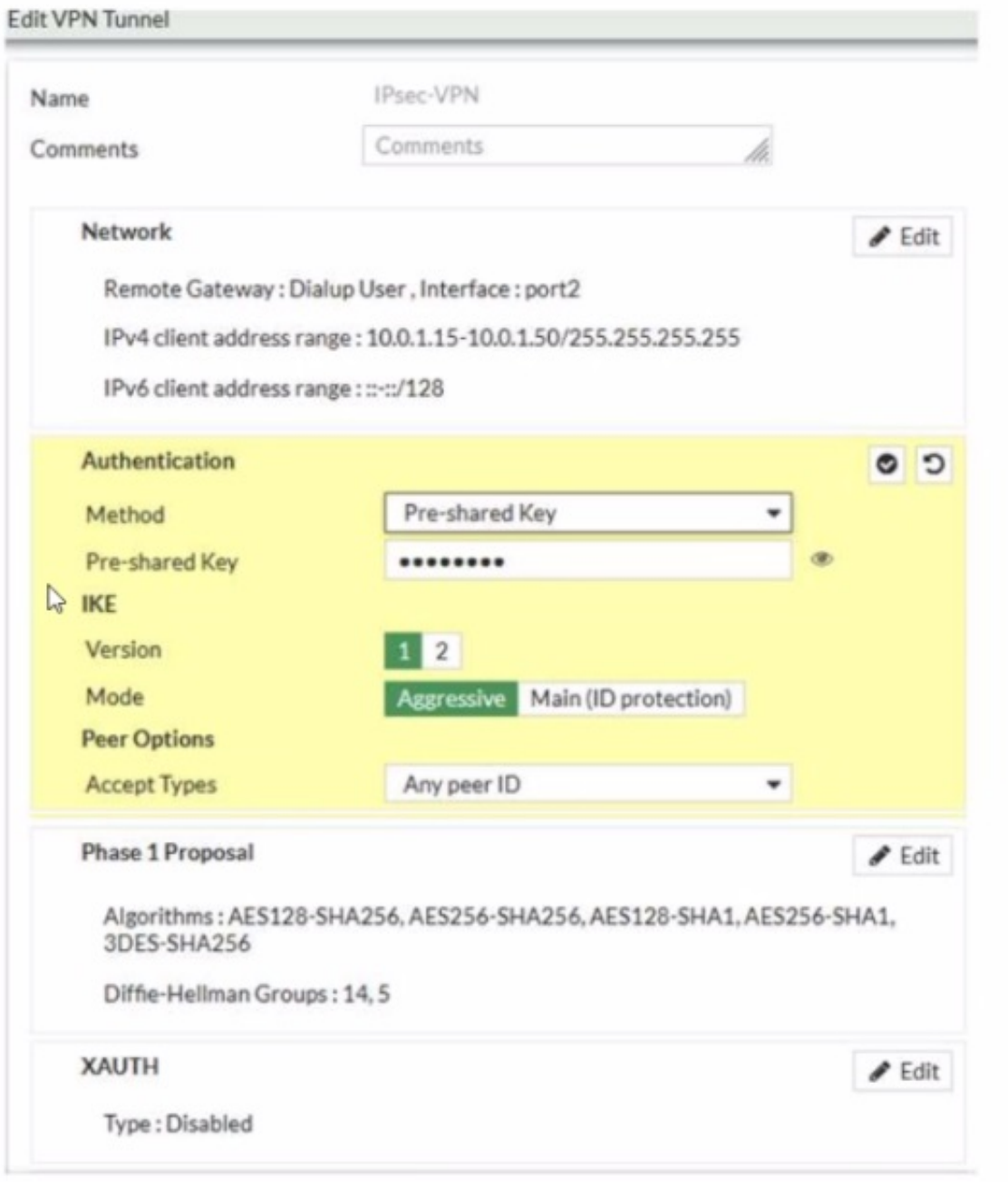

Examine the FortiGate user group configuration and the Windows AD LDAP group membership information shown in the exhibit
FortiGate is configured to authenticate SSL VPN users against Windows AD using LDAP The administrator configured the SSL VPN user group for SSL VPN users However the administrator 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 Nam© 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, “The 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.” 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.

**NEW QUESTION 19**
Refer to the exhibit.



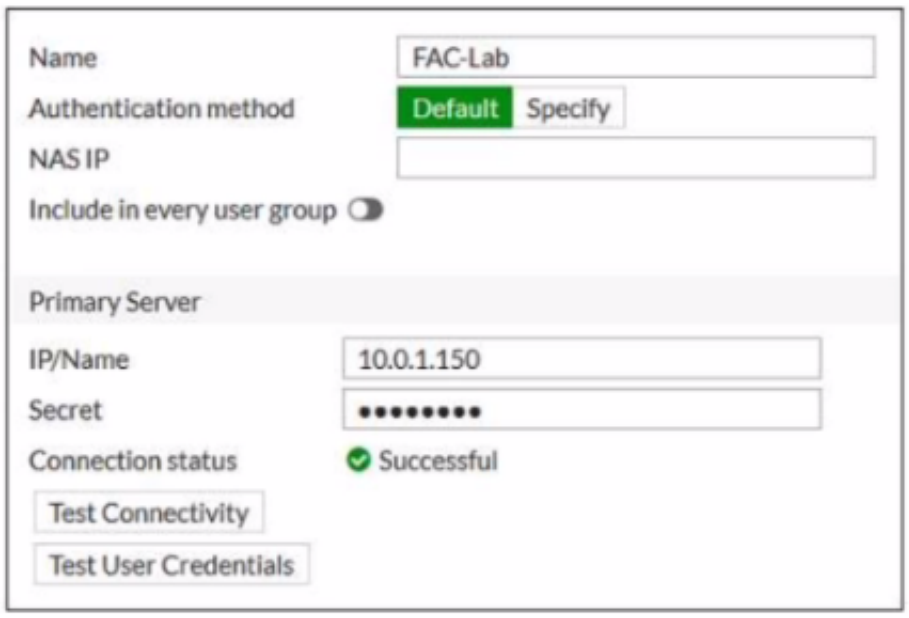

Examine the IPsec VPN phase 1 configuration shown in the exhibit
An administrator wants to use certificate-based authentication for an IPsec VPN user
Which three configuration changes must you make on FortiGate to perform certificate-based authentication for the IPsec VPN user? (Choose three)

A. Create a PKI user for the IPsec VPN user, and then configure the IPsec VPN tunnel to accept the PKI user as peer certificate
B. In the Authentication section of the IPsec VPN tunnel in the Method drop-down list select Signature and then select the certificate that FortiGate will use for IPsec VPN
C. In the IKE section of the IPsec VPN tunnel in the Mode field select Main (ID protection)
D. Import the CA that signed the user certificate
E. Enable XAUTH on the IPsec VPN tunnel

**Answer:** BDE

**Explanation:**
According to the FortiGate Administration Guide, “To use certificate-based authentication, you must configure the following settings on both peers: Select Signature as the authentication method and select a certificate to use for authentication. Import the CA certificate that issued the peer’s certificate. Enable XAUTH on the phase 1 configuration.” Therefore, options B, D, and E are true because they describe the configuration changes that must be made on FortiGate to perform certificate-based authentication for the IPsec VPN user. Option A is false because creating a PKI user for the IPsec VPN user is not required, as the user certificate can be verified by the CA certificate. Option C is false because changing the IKE mode to Main (ID protection) is not required, as the IKE mode can be either Main or Aggressive for certificate-based authentication.

**NEW QUESTION 24**
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 29**
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 32**
Refer to the exhibit.

```
FortiGate # diagnose test authserver radius FAC-Lab mschap2 student password
[1909] handle_req-Rcvd auth req 1288058912 for student in FAC-Lab opt=0000001d prot=4
[466] __compose_group_list_from_req-Group 'FAC-Lab', type 1
[617] fnbamd_pop3_start-student
[505] __fnbamd_cfg_get_radius_list_by_server-Loading RADIUS server 'FAC-Lab'
[342] fnbamd_create_radius_socket-Opened radius socket 13
[342] fnbamd_create_radius_socket-Opened radius socket 14
[1392] fnbamd_radius_auth_send-Compose RADIUS request
[1352] fnbamd_rad_dns_cb-10.0.1.150->10.0.1.150
[1330] __fnbamd_rad_send-Sent radius req to server 'FAC-Lab': fd=13, IP=10.0.1.150(10.0.1.150:1812) code=1 id=2 len=180 us
er="student" using MS-CHAPv2
[320] radius_server_auth-Timer of rad 'FAC-Lab' is added
  33] create_auth_session-Total 1 server(s) to try
  359] fnbamd_auth_handle_radius_result-Timer of rad 'FAC-Lab' is deleted
  800] fnbamd_radius_auth_validate_pkt-RADIUS resp code 2
[320] extract_success_vsas-FORTINET attr, type 1, val SSLVPN
[1661] __radius_decode_mppe_key-Key len after decode 16

[1661] __radius_decode_mppe_key-Key len after decode 16

[1385] fnbamd_auth_handle_radius_result-->Result for radius svr 'FAC-Lab' 10.0.1.150(1) is 0
[266] find_matched_usr_grps-Skipped group matching
[217] fnbamd_comm_send_result-Sending result 0 (nid 0) for req 1288058912, len=2156
authenticate 'student' against 'mschap2' succeeded, server=primary assigned_rad_session_id=1288058912 session_timeout=0 se
cs idle_timeout=0 secs'
Group membership(s) - SSLVPN
```

Examine the debug output shown in the exhibit
Which two statements about the RADIUS debug output are true" (Choose two)

A. The user student belongs to the SSLVPN group
B. User authentication failed
C. The RADIUS server sent a vendor-specific attribute in the RADIUS response
D. User authentication succeeded using MSCHAP

**Answer:** AD

**Explanation:**
According to the exhibit, the debug output shows a RADIUS debug output from FortiGate. The output shows that FortiGate sent a RADIUS Access-Request packet to FortiAuthenticator with the username student and received a RADIUS Access-Accept packet from FortiAuthenticator with a Class attribute containing SSLVPN. Therefore, option A is true because it indicates that the user student belongs to the SSLVPN group on FortiAuthenticator. The output also shows that FortiGate used MSCHAP as the authentication method and received a MS-MPPE-Send-Key and a MS-MPPE-Recv-Key from FortiAuthenticator. Therefore, option D is true because it indicates that user authentication succeeded using MSCHAP. Option B is false because user authentication did not fail, but rather succeeded. Option C is false because FortiAuthenticator did not send a vendor-specific attribute in the RADIUS response, but rather standard attributes defined by RFCs.

**NEW QUESTION 34**
.....

# 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