

# Fortinet

## Exam Questions NSE7\_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0



**NEW QUESTION 1**

Where can FortiGate learn the FortiManager IP address or FQDN for zero-touch provisioning'?

- A. From an LDAP server using a simple bind operation
- B. From a TFTP server
- C. From a DHCP server using options 240 and 241
- D. From a DNS server using A or AAAA records

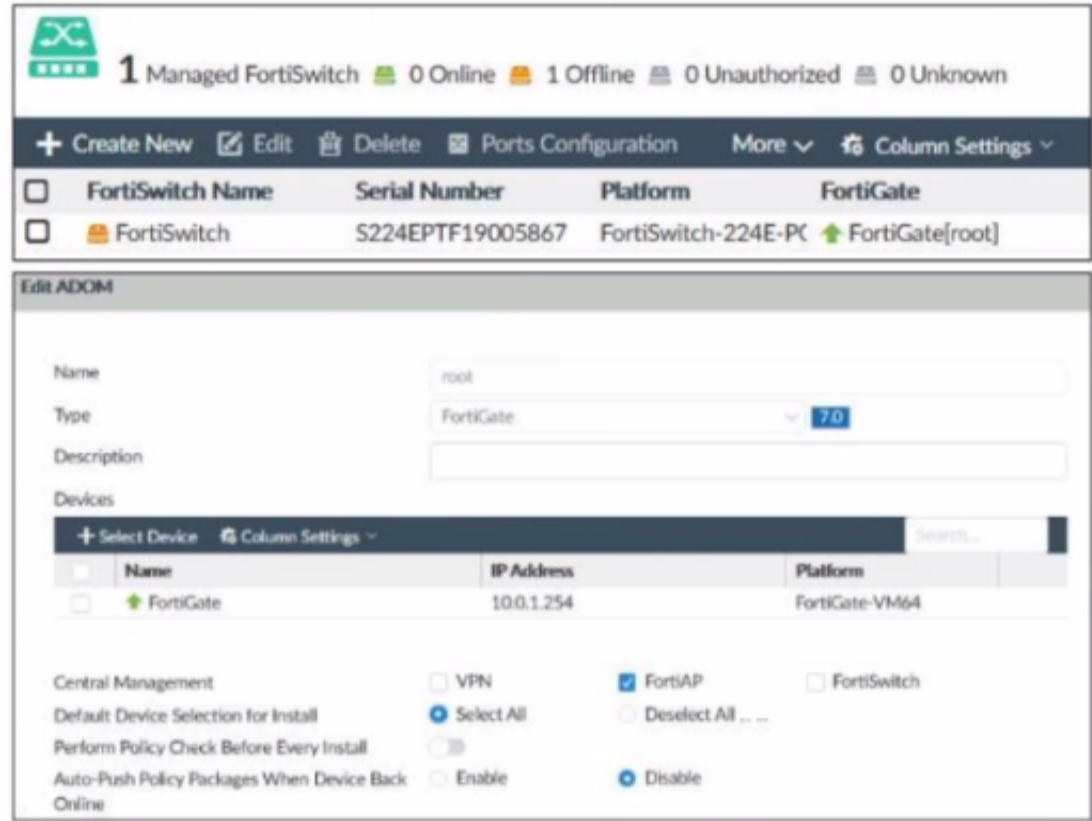
**Answer: D**

**Explanation:**

According to the FortiGate Administration Guide, “FortiGate can learn the FortiManager IP address or FQDN for zero-touch provisioning from a DNS server using A or AAAA records. The DNS server must be configured to resolve the hostname fortimanager.fortinet.com to the IP address or FQDN of the FortiManager device.” Therefore, option D is true because it describes the method for FortiGate to learn the FortiManager IP address or FQDN for zero-touch provisioning. Option A is false because LDAP is not used for zero-touch provisioning. Option B is false because TFTP is not used for zero-touch provisioning. Option C is false because DHCP options 240 and 241 are not used for zero-touch provisioning.

**NEW QUESTION 2**

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

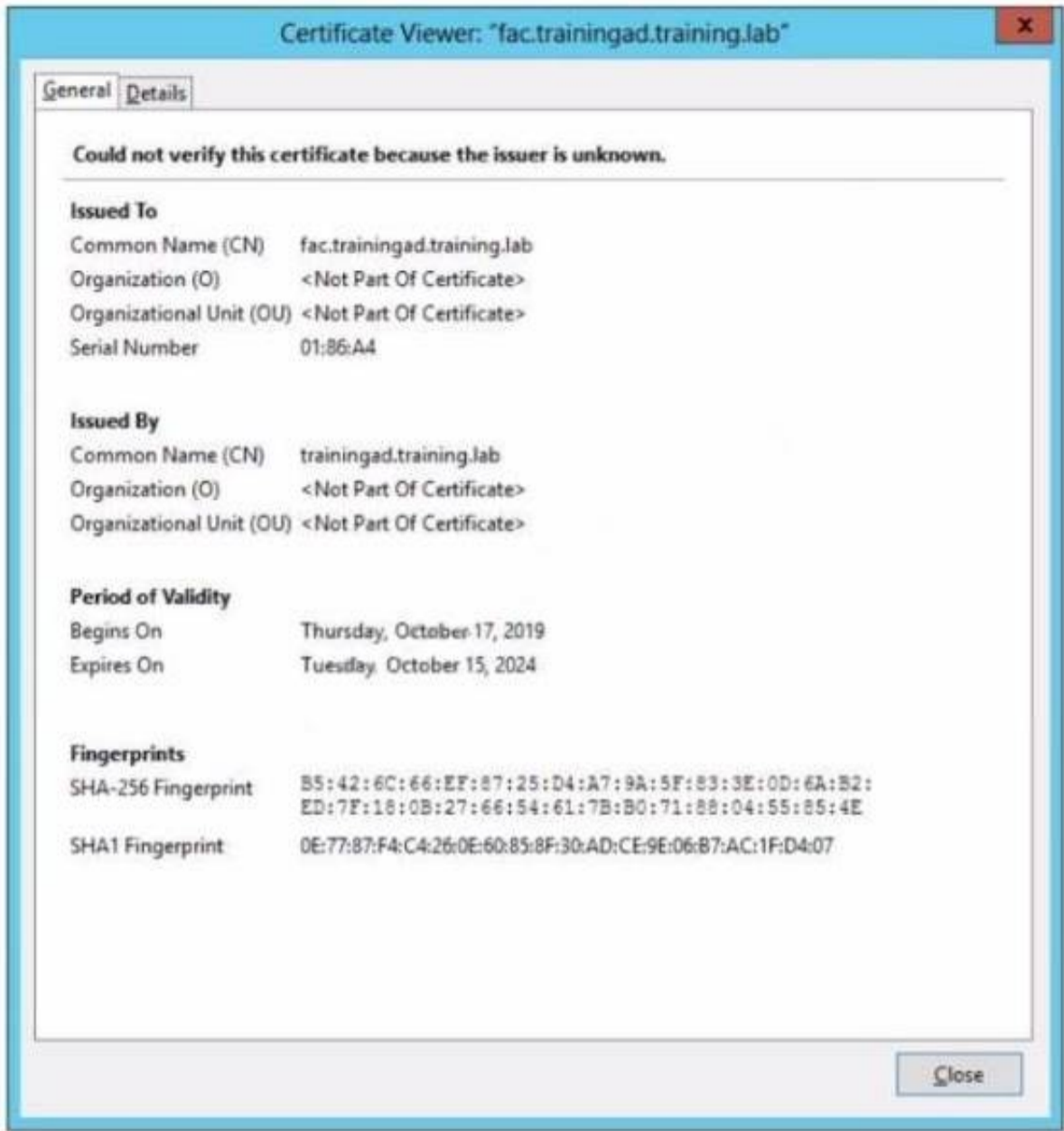
**Answer: CD**

**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.

**NEW QUESTION 3**

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

```
https://fac.trainingad.training.com/guest/login/?
loginpost=https://auth.trainingad.training.lab:1003/fqauthsmagic=000a030293d1f411&usermac=b8:27:eb:d8:50:72&ipmac=70:4c:a5:f5:0d:28&ip=10.10.100.2&userip=10.0.3.1&ssid=Guest03&apname=0822127718000148&ssid=70:4c:a5:9d:0d:30
```

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 4**

Refer to the exhibit

```
FortiGate # diagnose switch-controller switch-info 802.1X
Managed Switch : S224EPTF19006016

port2 : Mode: port-based (mac-by-pass disable)
Link: Link up
Port State: unauthorized: ( )
Dynamic Authorized Vlan : 0
Dynamic Allowed Vlan list:
Dynamic Untagged Vlan list:
EAP pass-through : Enable
EAP egress-frame-tagged : Enable
EAP auto-untagged-vlans : Enable
Allow MAC Move : Disable
Dynamic Access Control List : Disable
Quarantine VLAN (4093) detection : Enable
Native Vlan : 10
Allowed Vlan list: 10,4093
Untagged Vlan list: 4093
Guest VLAN :
Auth-Fail Vlan :
AuthServer-Timeout Vlan :

Sessions info:
00:09:0f:02:02:02      Type=802.1x,,state=AUTHENTICATING,etime=0,eap_cnt=0 params:reAuth=3600
```

A device connected to port2 on FortiSwitch cannot access the network The port is assigned a security policy to enforce 802 1X authentication While troubleshooting the issue, the administrator obtains the debug output shown in the exhibit Which two scenarios are likely to cause this issue? (Choose two.)

- A. The device is not configured for 802 1X authentication.
- B. The device has been quarantined for 3600 seconds.
- C. The device has been assigned the guest VLAN
- D. The device does not support 802 1X authentication

**Answer: AD**

#### Explanation:

According to the exhibit, the debug output shows that the device connected to port2 on FortiSwitch is sending an EAPOL-Start message, which is the first step of the 802.1X authentication process. However, the output also shows that the device is not sending any EAP-Response messages, which are required to complete the authentication process. Therefore, option A is true because the device is not configured for 802.1X authentication, which means that it does not have the correct credentials or settings to authenticate with the RADIUS server. Option D is also true because the device does not support 802.1X authentication, which means that it does not have the capability or software to perform 802.1X authentication. Option B is false because the device has not been quarantined for 3600 seconds, but rather has a session timeout of 3600 seconds, which is the default value for 802.1X sessions. Option C is false because the device has not been assigned the guest VLAN, but rather has been assigned the default VLAN, which is VLAN 1.

#### NEW QUESTION 5

Refer to the exhibit.

```
FortiGate # diagnose switch-controller switch-info mac-table S224EPTF19005047
Vdom: root
Managed Switch : S224EPTF19005047
MAC: 00:0c:29:e6:aad2 VLAN: 4089 Trunk: 0001V0000141803(trunk-id 0)
Flags: 0a00104e1 hit trunk dynamic src-hit native
MAC: 00:0c:29:e6:aad2 VLAN: 1 Trunk: 0001V0000141803(trunk-id 0)
Flags: 0a00104e1 hit trunk dynamic src-hit native
MAC: 00:0c:29:e6:aad2 VLAN: 4093 Trunk: 0001V0000141803(trunk-id 0)
Flags: 0a00104e1 hit trunk dynamic src-hit native
MAC: 00:0c:29:e6:aad2 VLAN: 4094 Trunk: 0001V0000141803(trunk-id 0)
Flags: 0a00104e1 hit trunk dynamic src-hit native
MAC: 70:8b:4b:5c:4a:0e VLAN: 9089 Ports: port2(post-id 2)
Flags: 0a00104e1 hit dynamic src-hit native
MAC: 04:d1:90:3a:e7:00 VLAN: 1 Ports: port1(post-id 1)
Flags: 0a00104e1 hit dynamic src-hit native
MAC: 00:0c:29:e6:aad2 VLAN: 4089 Trunk: 0001V0000141803(trunk-id 0)
Flags: 0a00104e1 hit trunk dynamic src-hit native
MAC: 00:0c:29:e6:aad2 VLAN: 1 Trunk: 0001V0000141803(trunk-id 0)
Flags: 0a00104e1 hit trunk dynamic src-hit native
Total Displayed: 8

FortiGate # diagnose switch-controller mac-device mac onboarding
Vdom: root
VLAN MAC LAST-SEEN TYPE LOCATION
4089 70:8b:4b:5c:4a:0e 4 DM S224EPTF19005047 port2

FortiGate # diagnose switch-controller mac-device mac known
Vdom: root
MAC LAST-KNOWN-SWITCH LAST-KNOWN-PORT MATCHED-MAC-POLICY MAC-POLICY-ACTION LAST-SEEN FEM-ID COMMENTS
FortiGate #
```

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 in 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: AB**

**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”.

**NEW QUESTION 6**

Which two statements about the MAC-based 802.1X security mode available on FortiSwitch are true? (Choose two.)

- A. FortiSwitch authenticates a single device and opens the port to other devices connected to the port
- B. FortiSwitch authenticates each device connected to the port
- C. It cannot be used in conjunction with MAC authentication bypass
- D. FortiSwitch can grant different access levels to each device connected to the port

**Answer: BD**

**Explanation:**

According to the FortiSwitch Administration Guide, “MAC-based 802.1X security mode allows you to authenticate each device connected to a port using its MAC address as the username and password.” Therefore, option B is true because it describes the MAC-based 802.1X security mode available on FortiSwitch. Option D is also true because FortiSwitch can grant different access levels to each device connected to the port based on the user group and security policy assigned to them. Option A is false because FortiSwitch does not authenticate a single device and open the port to other devices connected to the port, but rather authenticates each device individually. Option C is false because MAC-based 802.1X security mode can be used in conjunction with MAC authentication bypass (MAB) or EAP pass-through modes, which are fallback options for non-802.1X devices.

**NEW QUESTION 7**

A wireless network in a school provides guest access using a captive portal to allow unregistered users to self-register and access the network. The administrator is requested to update the existing configuration to provide captive portal authentication through a secure connection (HTTPS).

Which two changes must the administrator make to enforce HTTPS authentication"? (Choose two >

- A. Create a new SSID with the HTTPS captive portal URL
- B. Enable HTTP redirect in the user authentication settings
- C. Disable HTTP administrative access on the guest SSID to enforce HTTPS connection
- D. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator

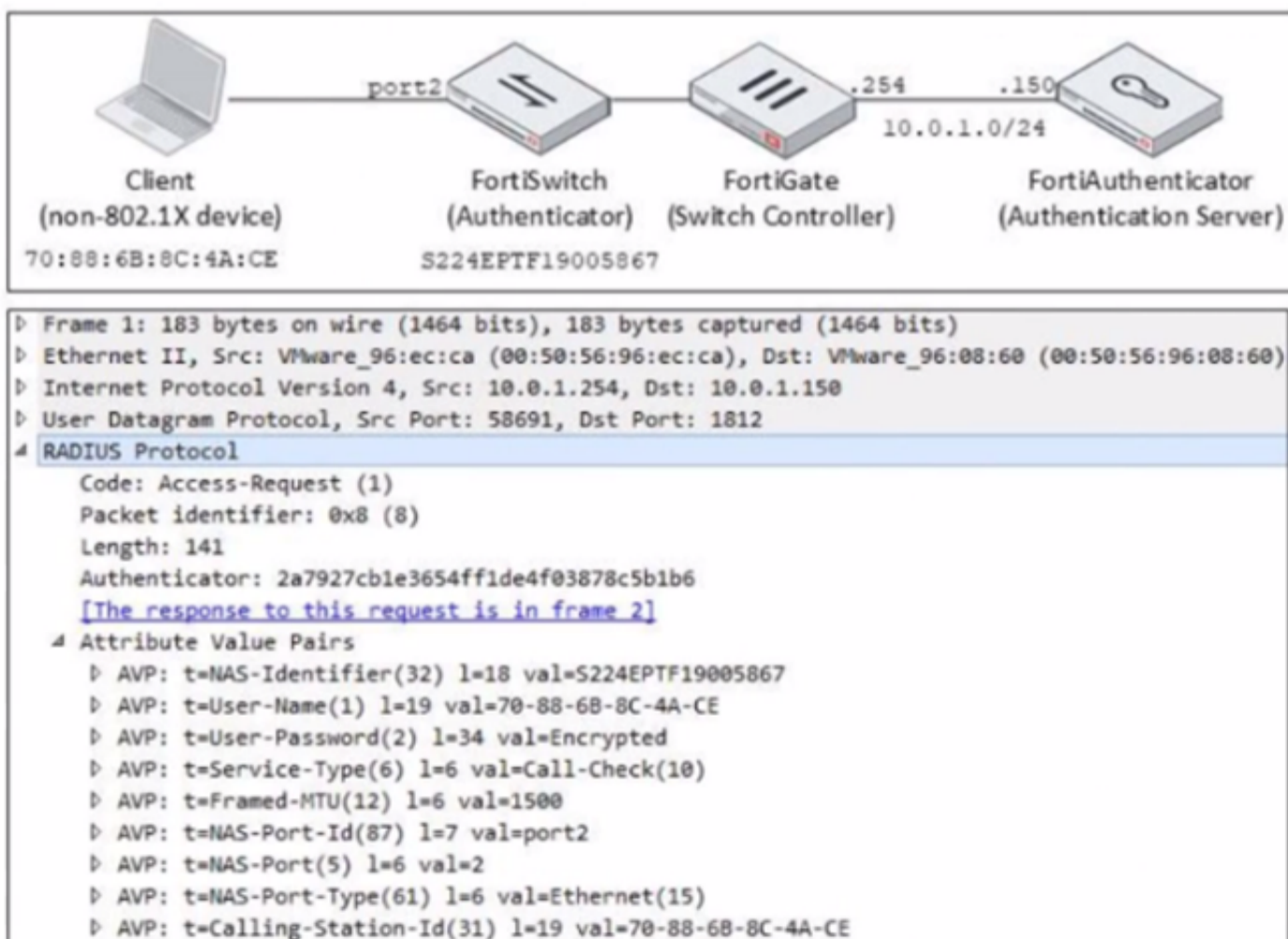
**Answer: BD**

**Explanation:**

According to the FortiGate Administration Guide, “To enable HTTPS authentication, you must enable HTTP redirect in the user authentication settings. This redirects HTTP requests to HTTPS. You must also update the captive portal URL to use HTTPS on both FortiGate and FortiAuthenticator.” Therefore, options B and D are true because they describe the changes that the administrator must make to enforce HTTPS authentication for the captive portal. Option A is false because creating a new SSID with the HTTPS captive portal URL is not required, as the existing SSID can be updated with the new URL. Option C is false because disabling HTTP administrative access on the guest SSID will not enforce HTTPS connection, but rather block HTTP connection.

**NEW QUESTION 8**

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

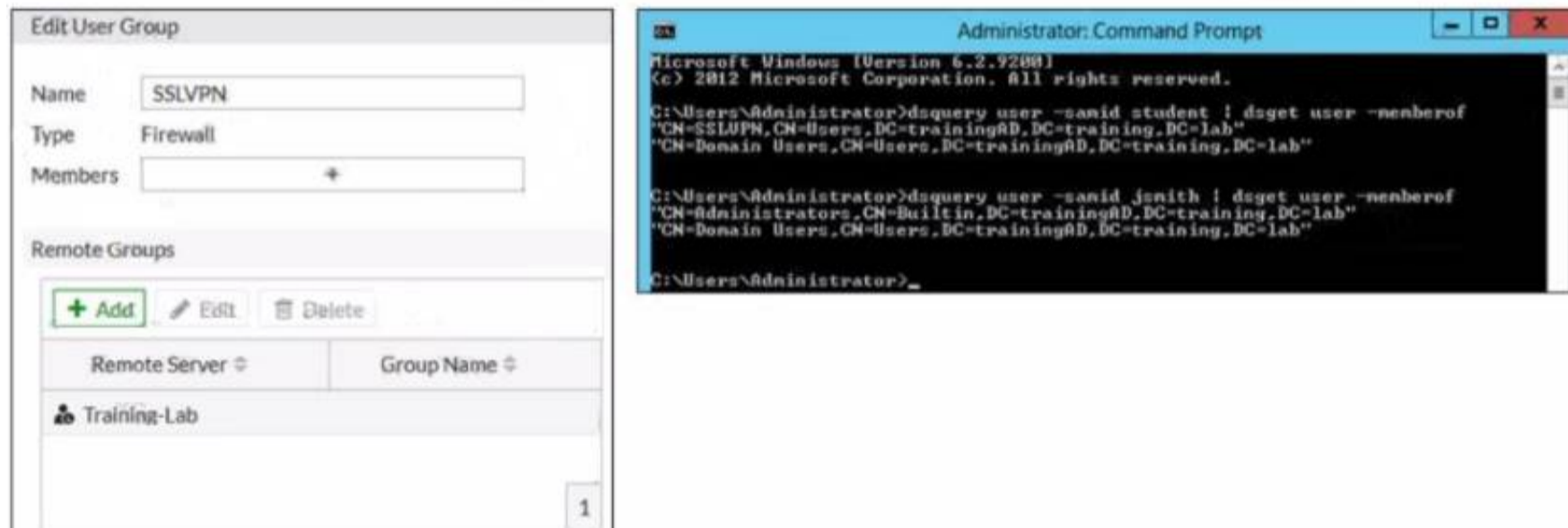
**Answer: B**

**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 9**

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 jsmith 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 Name 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, DC=training, 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 10**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE7\\_LED-7.0 Practice Test Here](#)**