

# Fortinet

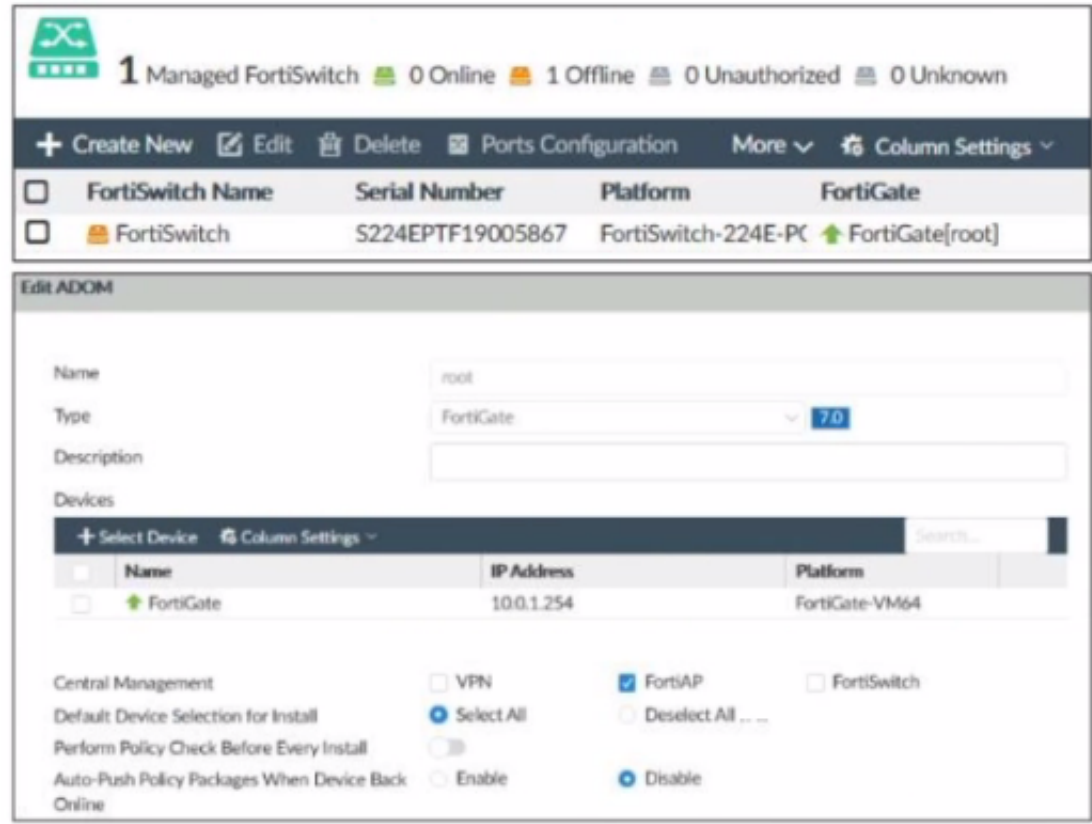
## Exam Questions NSE7\_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0



NEW QUESTION 1

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

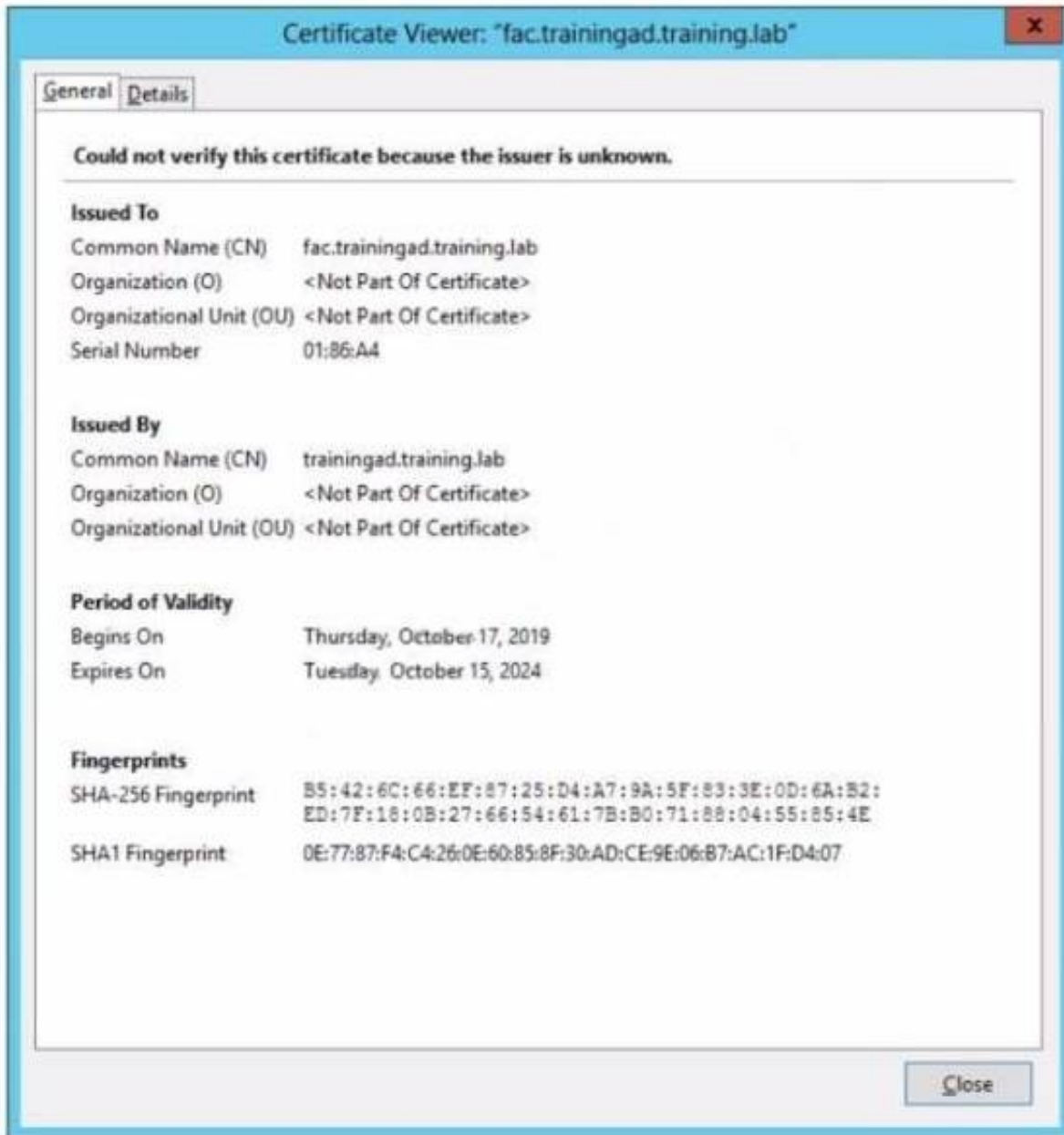
Answer: CD

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 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

```
https://fac.trainingad.training.com/guest/login/?
loginpost=https://auth.trainingad.training.lab/1003/fqauthmagic=00a030293d1f411ausermac=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=082212771800014&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 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 MAC address 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.

The screenshot displays the FortiGate configuration interface. At the top, there are two widgets: 'Security Fabric Setup' (Training) and 'FortiAnalyzer Logging' (10.0.1.210). Below these, the 'Edit Automation Stitch' section shows a configuration for an automation stitch named 'IOC'. The status is 'Enable', and the FortiGate(s) are set to 'All FortiGates'. The action execution is set to 'Sequential'. The stitch is triggered by a 'Compromised Host - High' event, followed by an 'Add delay' step, and then an 'Action' step: 'Quarantine on FortiSwitch + FortiAP'. Below the stitch configuration, there is a 'Quarantine' widget showing 'No results'. To the right, the 'FortiAnalyzer Logs' table is visible, showing two log entries for blocked HTTP requests to malicious websites.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
Internet	all	all	always	ALL	ACCEPT	Enabled	web default, certificate-inspection	All

#	Date/Time	Device ID	User	Source	Destination IP	Service	Host Name	Action	URL	Category	Description
1	11:16:29	FGVM1V000014...		10.0.2.2	10.0.2.17	HTTP	abcommuni	blocked	http://abcommuni/	Malicious Websites	
2	11:16:29	FGVM1V000014...		10.0.2.2	10.0.2.17	HTTP	abcommuni	blocked	http://abcommuni/favicon.ico	Malicious Websites	

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 (10.0.2.2) is connected to a managed FortiSwitch device. 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**

Which two statements about FortiSwitchmanager are true? (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 Guide, "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 guide, "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 any switch 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 6**

You are investigating a report of poor wireless performance in a network that you manage. The issue is related to an AP interface in the 5 GHz range. You are monitoring the channel utilization over time.

What is the recommended maximum utilization value that an interface should not exceed?

- A. 85%
- B. 95%
- C. 75%
- D. 65%

**Answer: D**

**Explanation:**

According to the FortiAP Configuration Guide, “Channel utilization measures how busy a channel is over a given period of time. It includes both Wi-Fi and non-Wi-Fi interference sources. A high channel utilization indicates a congested channel and can result in poor wireless performance. The recommended maximum utilization value that an interface should not exceed is 65%.” Therefore, option D is true because it gives the recommended maximum utilization value for an interface in the 5 GHz range. Options A, B, and C are false because they give higher utilization values that can cause poor wireless performance.  
<https://docs.fortinet.com/document/fortiap/7.0.0/configuration-guide/734537/wireless-radio-settings#channel-uti>

**NEW QUESTION 7**

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 8**

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 9**

You are setting up an SSID (VAP) to perform RADIUS-authenticated dynamic VLAN allocation. Which three RADIUS attributes must be supplied by the RADIUS server to enable successful VLAN allocation? (Choose three.)

- A. Tunnel-Private-Group-ID
- B. Tunnel-Pvt-Group-ID
- C. Tunnel-Preference
- D. Tunnel-Type
- E. Tunnel-Medium-Type

**Answer:** ADE

**Explanation:**

According to the FortiAP Configuration Guide, "To perform RADIUS-authenticated dynamic VLAN allocation, the RADIUS server must supply the following RADIUS attributes: Tunnel-Private-Group-ID, which specifies the VLAN ID to assign to the user. Tunnel-Type, which specifies the tunneling protocol used for the VLAN. The value must be 13 (VLAN). Tunnel-Medium-Type, which specifies the transport medium used for the VLAN. The value must be 6 (802). Therefore, options A, D, and E are true because they describe the RADIUS attributes that must be supplied by the RADIUS server to enable successful VLAN allocation. Option B is false because Tunnel-Pvt-Group-ID is not a valid RADIUS attribute name, but rather a typo for Tunnel-Private-Group-ID. Option C is false because Tunnel-Preference is not a required RADIUS attribute for dynamic VLAN allocation, but rather an optional attribute that specifies the priority of the VLAN.

**NEW QUESTION 10**

Refer to the exhibit.

The screenshot displays the FortiManager configuration for a NAC Policy named 'Training'. The policy is enabled and associated with FortiSwitch1. The device pattern is set to '70B84b5c4a0b' (Device: 70B84b5c4a0b, User: EHS-Tag, OS: Linux). The switch controller action is set to 'Assign VLAN' with 'Students' as the source port. The right pane shows the FortiGate CLI output for 'diagnose switch-controller mac-table' and 'diagnose switch-controller mac-device mac onboarding', both showing the device as not matching the policy.

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: 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 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**

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**

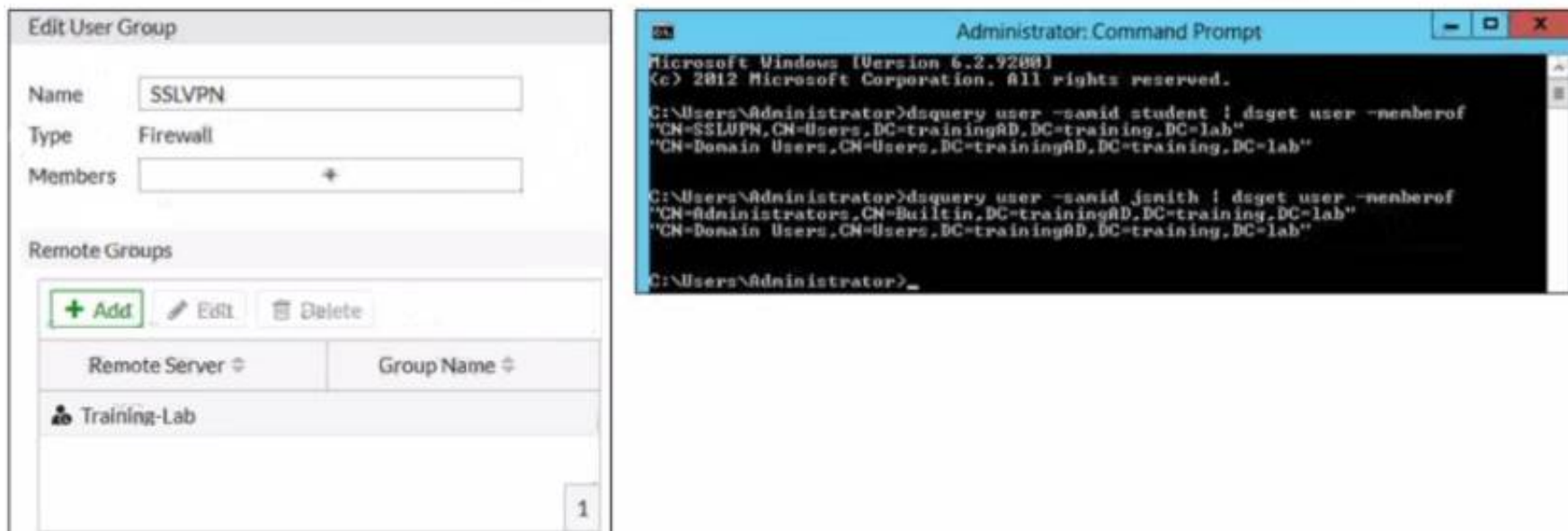
**Explanation:**

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 15

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 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 Guide, "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 24

.....



## 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](#)**