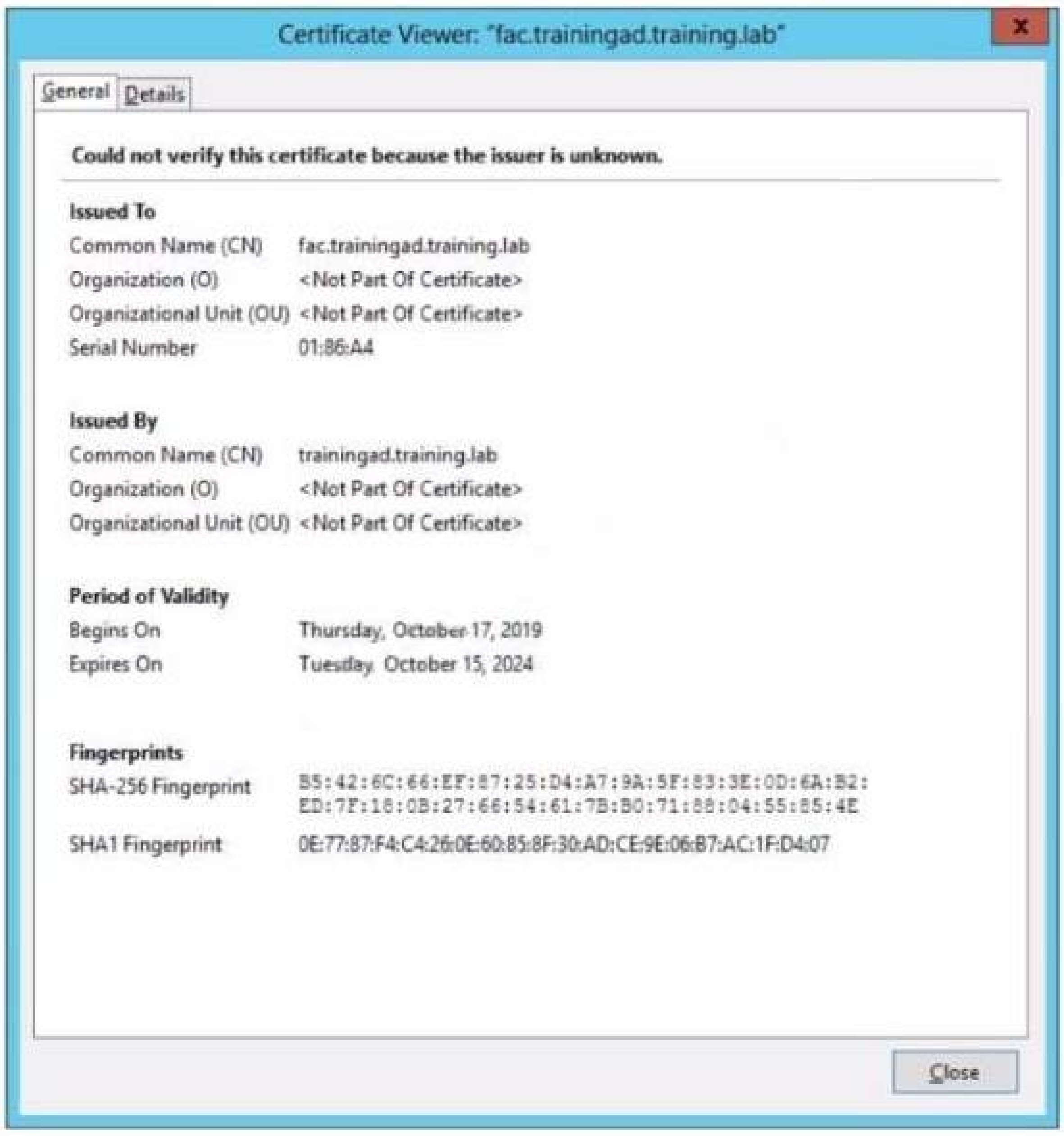
Exam Questions NSE7_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0

https://www.2passeasy.com/dumps/NSE7_LED-7.0/

NEW QUESTION 1
Refer to the exhibit



Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	fac.trainingad.training.lab
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	01:86:A4

Issued By

Common Name (CN)	trainingad.training.lab
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

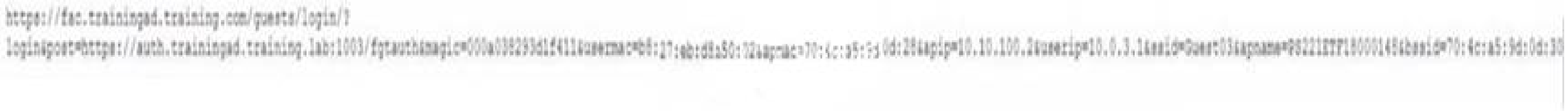
Period of Validity

Begins On	Thursday, October 17, 2019
Expires On	Tuesday, October 15, 2024

Fingerprints

SHA-256 Fingerprint	B5:42:6C:66:EF:87:25:D4:A7:9A:5F:83:3E:0D:6A:B2: ED:7F:16:0B:27:66:54:61:7B:B0:71:88:04:55:85:4E
SHA1 Fingerprint	0E:77:87:F4:C4:26:0E:60:85:8F:30:AD:CE:9E:06:B7:AC:1F:D4:07

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/guests/login/?
loginpost=https://auth.trainingad.training.lab:1003/fgtauth&magic=000a038293d1f411&usermac=b8:27:eb:d8a50:32&apmac=70:4c:a5:9d:0d:28&apip=10.10.100.2&userip=10.0.3.1&ssid=Guest03&apname=FP221ETF18000148&bssid=70:4c:a5:9d:0d:30
```

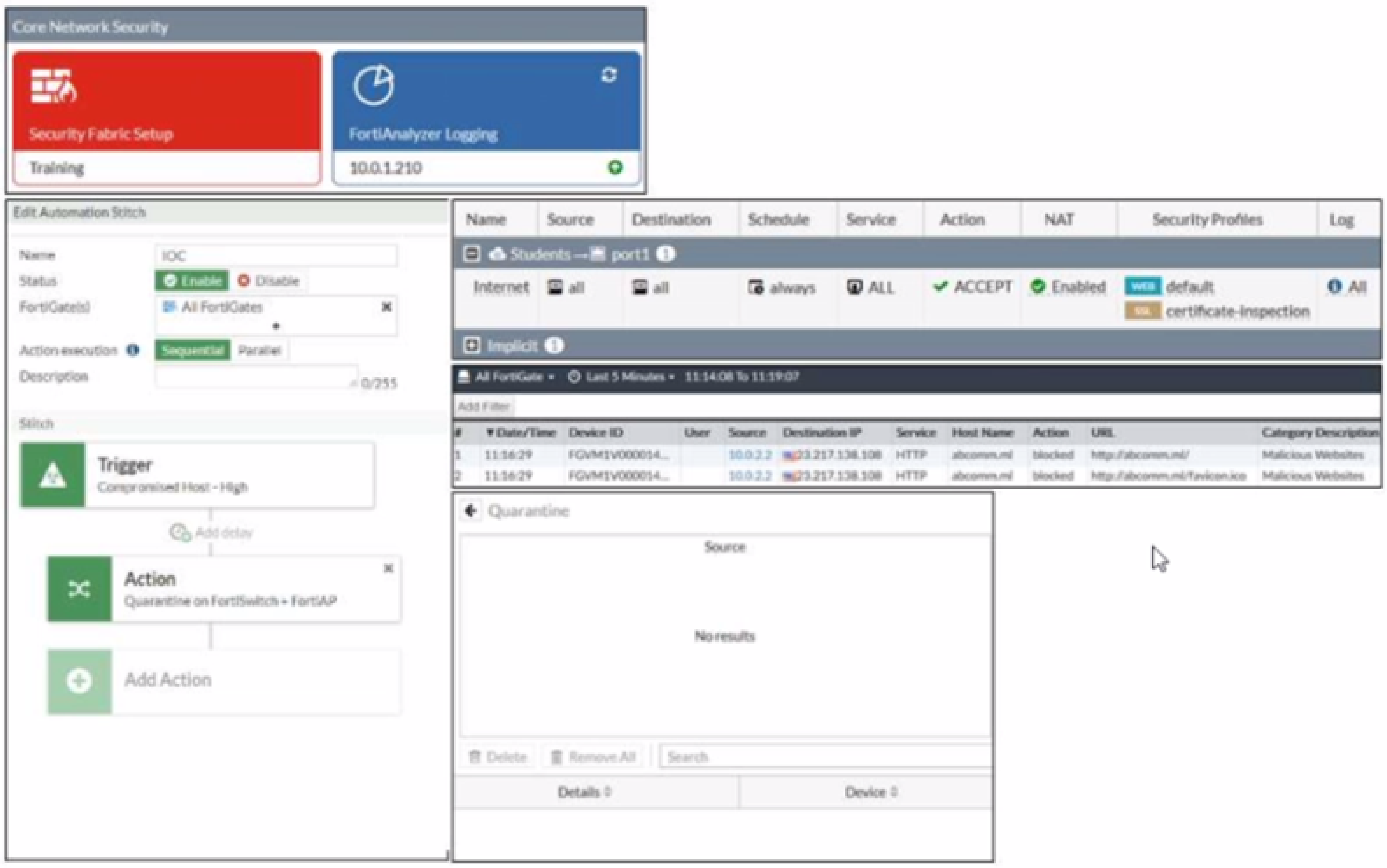
Which two settings are the likely causes of the issue? (Choose two.)

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 2
Refer to the exhibit.



Core Network Security

Security Fabric Setup: Training

FortiAnalyzer Logging: 10.0.1.210

Edit Automation Stitch

Name	IOC
Status	Enable / Disable
FortiGate(s)	All FortiGates
Action execution	Sequential / Parallel
Description	0/255

Stitch

Trigger: Compromised Host - High

Add delay

Action: Quarantine on FortiSwitch + FortiAP

Add Action

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
Students → port1 1								
Internet	all	all	always	ALL	✓ ACCEPT	Enabled	WEB default SSL certificate-inspection	All
Implicit 1								

All FortiGate ▾ Last 5 Minutes ▾ 11:14:08 To 11:19:07

Add Filter

#	Date/Time	Device ID	User	Source	Destination IP	Service	Host Name	Action	URL	Category Description
1	11:16:29	FGVM1V000014...		10.0.2.2	23.217.138.108	HTTP	abcomm.ml	blocked	http://abcomm.ml/	Malicious Websites
2	11:16:29	FGVM1V000014...		10.0.2.2	23.217.138.108	HTTP	abcomm.ml	blocked	http://abcomm.ml/favicon.ico	Malicious Websites

Quarantine

Source

No results

Delete | Remove All | Search

Details | Device

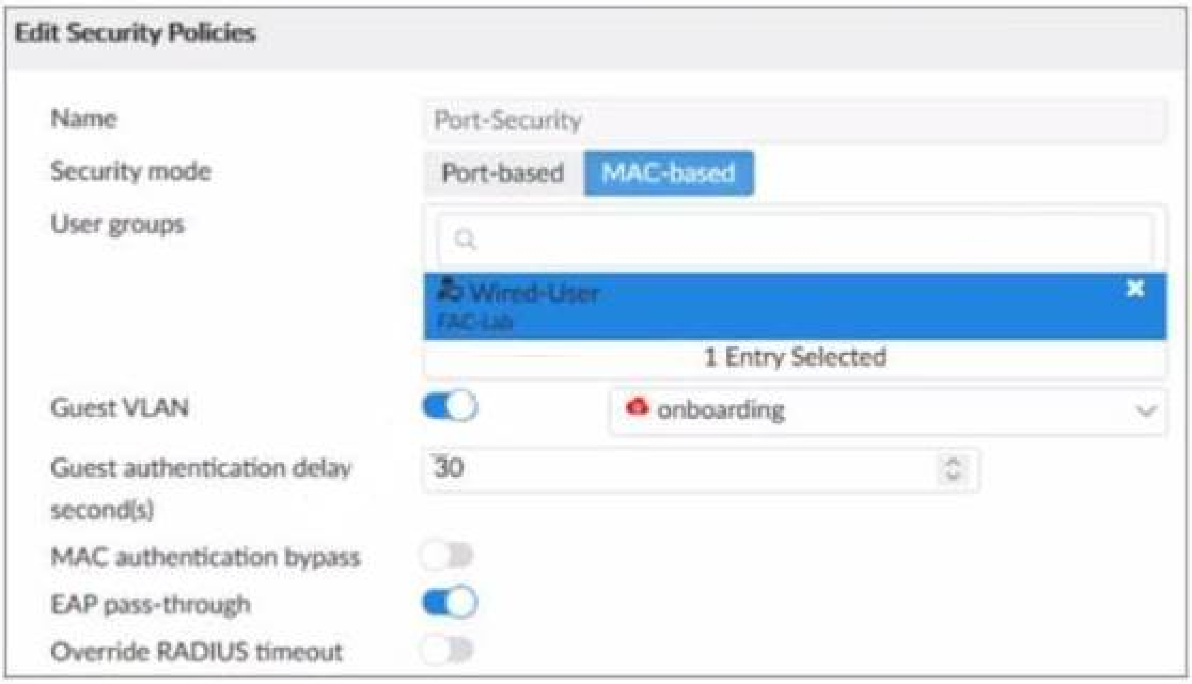
Examine the FortiGate configuration FortiAnalyzer logs and FortiGate widget shown in the exhibit
An administrator is testing the Security Fabric quarantine automation The administrator added FortiAnalyzer to the Security Fabric and configured an automation stitch to automatically quarantine compromised 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 3
Refer to the exhibit.



Edit Security Policies

Name	Port-Security
Security mode	Port-based / MAC-based
User groups	Wired-User FAC-Lab 1 Entry Selected
Guest VLAN	● onboarding
Guest authentication delay second(s)	30
MAC authentication bypass	○
EAP pass-through	●
Override RADIUS timeout	○

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 4
What is the purpose of enabling Windows Active Directory Domain Authentication on FortiAuthenticator?

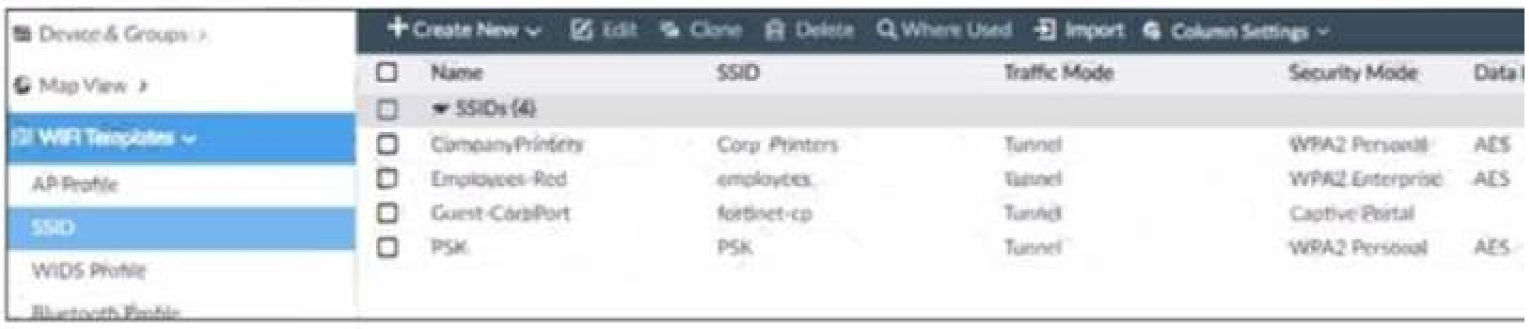
A. It enables FortiAuthenticator to use Windows administrator credentials to perform an LDAP lookup for a user search
B. It enables FortiAuthenticator to use a Windows CA certificate when authenticating RADIUS users
C. It enables FortiAuthenticator to import users from Windows AD
D. It enables FortiAuthenticator to register itself as a Windows trusted device to proxy authentication using Kerberos

Answer: D

Explanation:
According to the FortiAuthenticator Administration Guide2, “Windows Active Directory domain authentication enables FortiAuthenticator to join a Windows Active Directory domain as a machine entity and proxy authentication requests using Kerberos.” Therefore, option D is true because it describes the purpose of enabling Windows Active Directory domain authentication on FortiAuthenticator. Option A is false because FortiAuthenticator does not need Windows administrator credentials to perform an LDAP lookup for a user search. Option B is false because FortiAuthenticator does not use a Windows CA certificate when authenticating RADIUS users, but rather its own CA certificate. Option C is false because FortiAuthenticator does not import users from Windows AD, but rather synchronizes them using LDAP or FSSO.

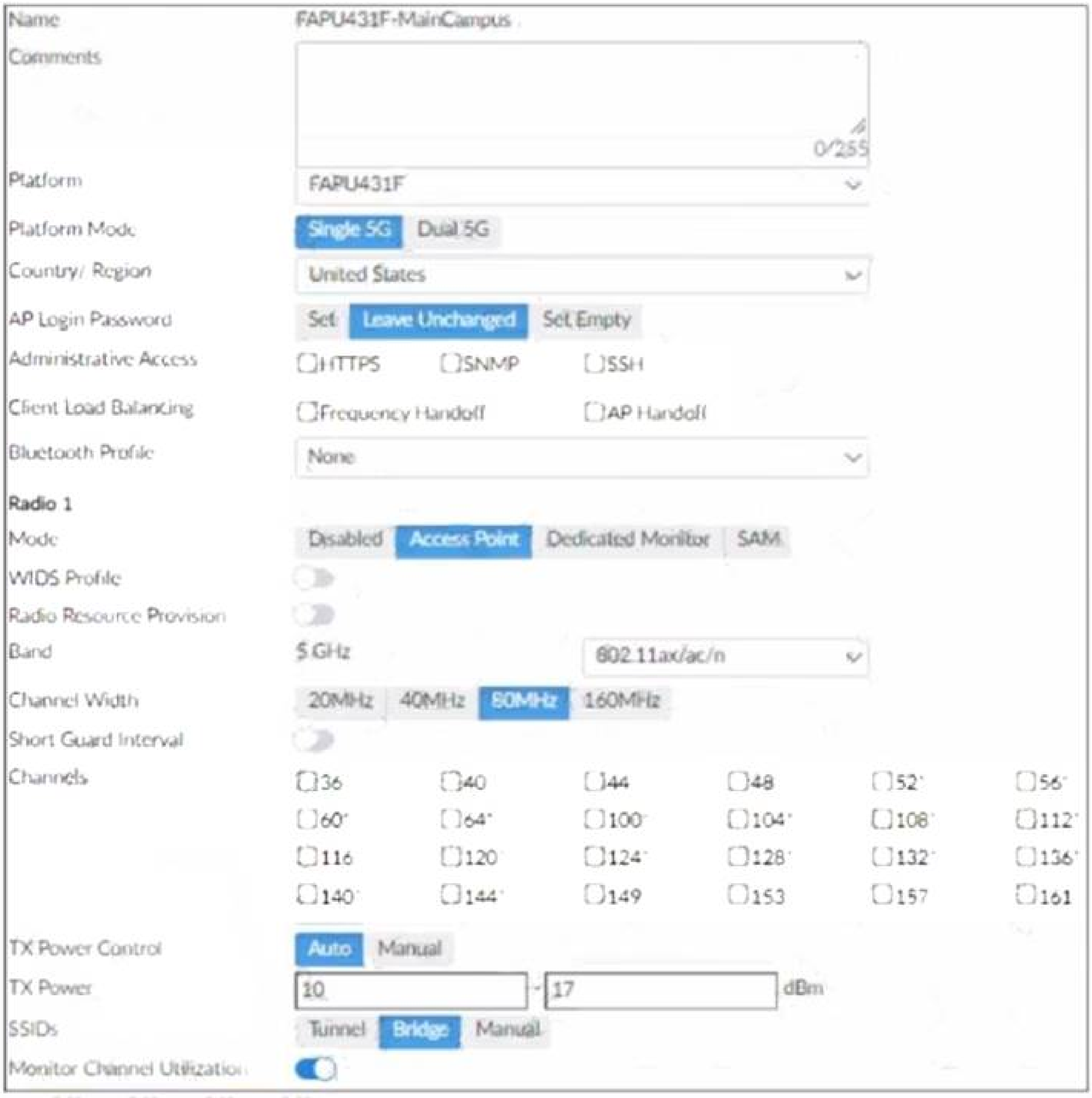
NEW QUESTION 5
Refer to the exhibits

SSID Profiles



□	Name	SSID	Traffic Mode	Security Mode	Data
□	SSIDs (4)				
□	CompanyPrinters	Corp Printers	Tunnel	WPA2 Personal	AES
□	Employees-Red	employees	Tunnel	WPA2 Enterprise	AES
□	Guest-CorpPort	fortinet-cp	Tunnel	Captive Portal	
□	PSK	PSK	Tunnel	WPA2 Personal	AES

AP Profile



Name	FAPU431F-MainCampus
Comments	0/255
Platform	FAPU431F
Platform Mode	[✓ Single 5G] Dual 5G
Country/ Region	United States
AP Login Password	Set [✓ Leave Unchanged] Set Empty
Administrative Access	□ HTTPS □ SNMP □ SSH
Client Load Balancing	□ Frequency Handoff □ AP Handoff
Bluetooth Profile	None
Radio 1	
Mode	Disabled [✓ Access Point] Dedicated Monitor SAM
WIDS Profile	○
Radio Resource Provision	○
Band	5 GHz 802.11ax/ac/n
Channel Width	20MHz 40MHz [✓ 80MHz] 160MHz
Short Guard Interval	○
Channels	□36 □40 □44 □48 □52* □56* □60* □64* □100* □104* □108* □112* □116 □120* □124* □128* □132* □136* □140* □144* □149 □153 □157 □161
TX Power Control	[✓ Auto] Manual
TX Power	10 - 17 dBm
SSIDs	Tunnel [✓ Bridge] Manual
Monitor Channel Utilization	●

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 SSlDs 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 6
You are setting up an SSID (VAP) to perform RADlUS-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 7
An administrator is testing the connectivity for a new VLAN The devices in the VLAN are connected to a FortiSwitch device that is managed by FortiGate Quarantine is disabled on FortiGate
While testing the administrator noticed that devices can ping FortiGate and FortiGate can ping the devices The administrator also noticed that inter-VLAN communication works However intra-VLAN communication does not work
Which scenario is likely to cause this issue?

A. Access VLAN is enabled on the VLAN
B. The native VLAN configured on the ports is incorrect
C. The FortiSwitch MAC address table is missing entries
D. The FortiGate ARP table is missing entries

Answer: C

Explanation:
According to the scenario, the devices in the VLAN are connected to a FortiSwitch device that is managed by FortiGate. Quarantine is disabled on FortiGate, which means that the devices are not blocked by any security policy. The devices can ping FortiGate and FortiGate can ping the devices, which means that the IP connectivity is working. Inter-VLAN communication works, which means that the routing between VLANs is working. However, intra-VLAN communication does not work, which means that the switching within the VLAN is not working. Therefore, option C is true because the FortiSwitch MAC address table is missing entries, which means that the FortiSwitch does not know how to forward frames to the destination MAC addresses within the VLAN. Option A is false because access VLAN is enabled on the VLAN, which means that the VLAN ID is added to the frames on ingress and removed on egress. This does not affect intra-VLAN communication. Option B is false because the native VLAN configured on the ports is incorrect, which means that the frames on the native VLAN are not tagged with a VLAN ID. This does not affect intra-VLAN communication. Option D is false because the FortiGate ARP table is missing entries, which means that FortiGate does not know how to map IP addresses to MAC addresses. This does not affect intra-VLAN communication.

NEW QUESTION 8
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 9
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.

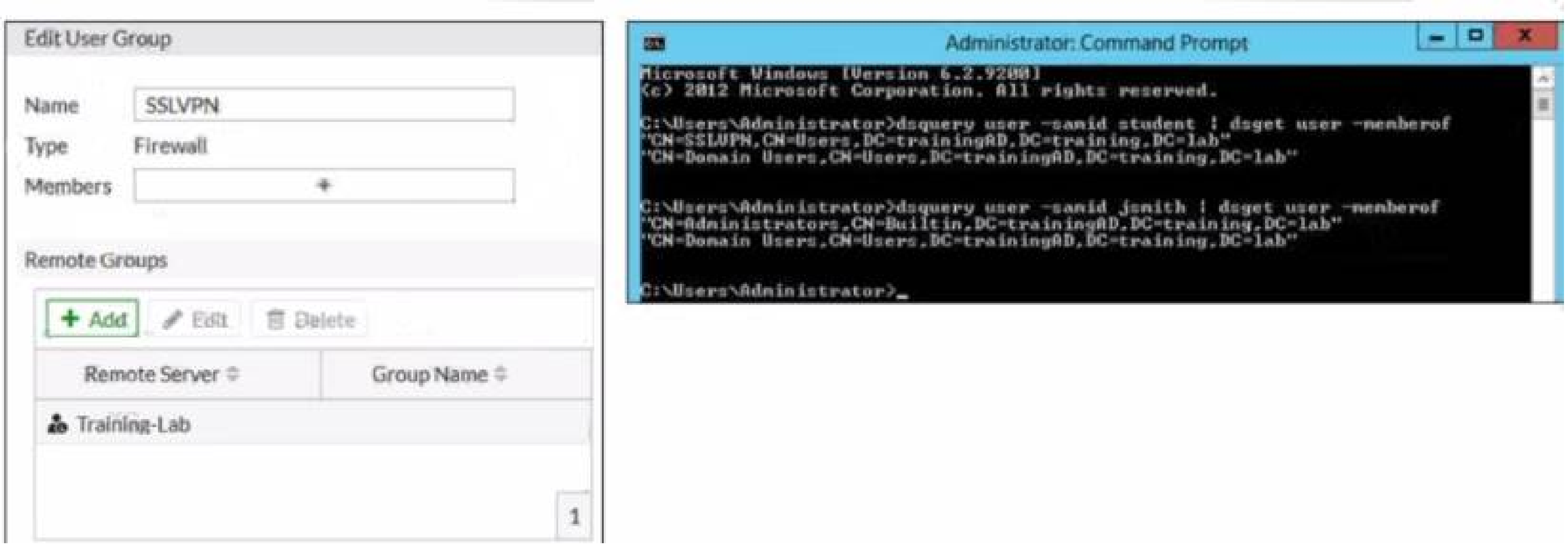
NEW QUESTION 10
A wireless network in a school provides guest access using a captive portal to allow unregistered users to self-register and access the network The administrator is requested to update the existing configuration to provide captive portal authentication through a secure connection (HTTPS)
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 14
Refer to the exhibit.



Name: SSLVPN
Type: Firewall
Members:

Remote Groups

Remote Server	Group Name
Training-Lab	

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dsquery user -samid student | dsget user -memberof
"CN=SSLVPN,CN=Users,DC=trainingAD,DC=training,DC=lab"
"CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab"

C:\Users\Administrator>dsquery user -samid jsmith | dsget user -memberof
"CN=Administrators,CN=Builtin,DC=trainingAD,DC=training,DC=lab"
"CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab"

C:\Users\Administrator>_
```

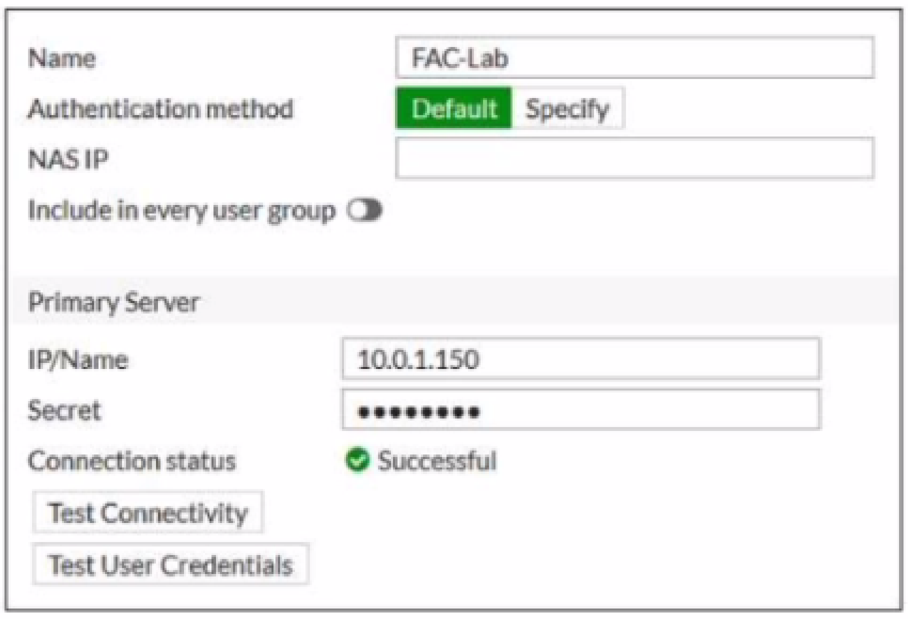
Examine the FortiGate user group configuration and the Windows AD LDAP group membership information shown in the exhibit
FortiGate is configured to authenticate SSL VPN users against Windows AD using LDAP The administrator configured the SSL VPN user group for SSL VPN users However the administrator 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 17
Refer to the exhibit.



Name	FAC-Lab
Authentication method	Default Specify
NAS IP	
Include in every user group	○

Primary Server

IP/Name	10.0.1.150
Secret	●●●●●●●●●
Connection status	✓ Successful

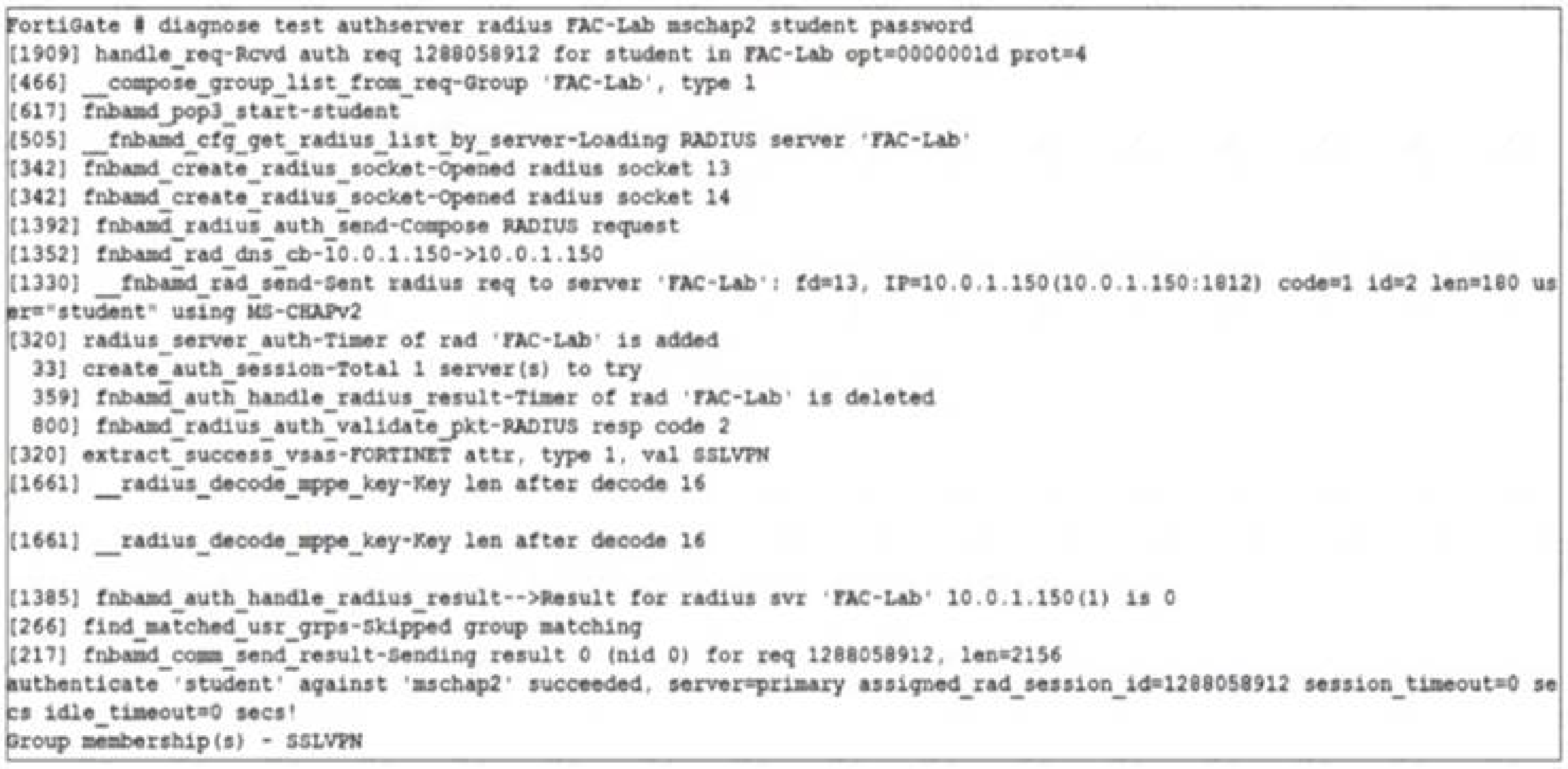
Examine the RADIUS server configuration shown in the exhibit
An administrator has configured a RADIUS server on FortiGate that points to FortiAuthenticator FortiAuthenticator is acting as an authentication proxy and is configured to relay all authentication requests to a remote Windows AD server using 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 18
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 20

......