Vendor: Fortinet

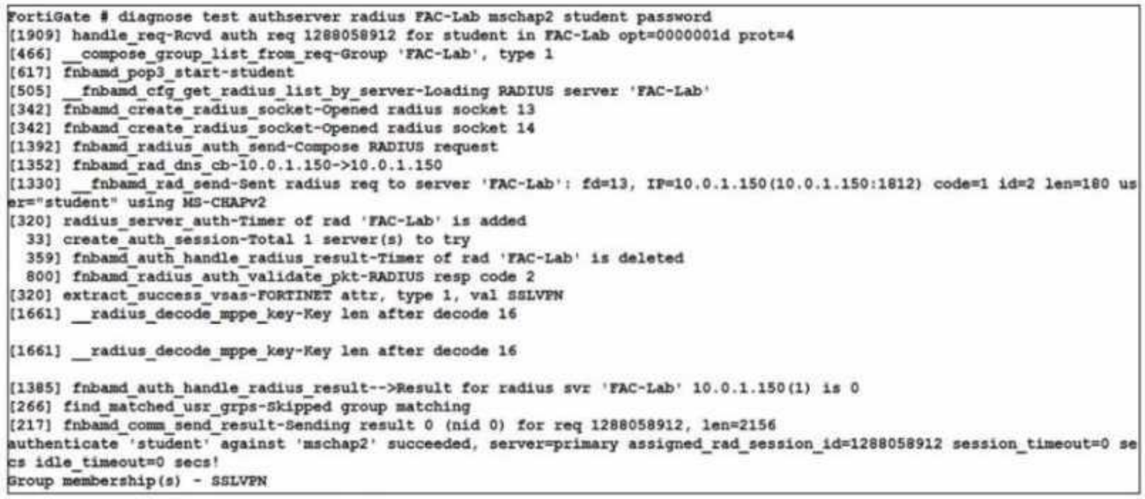
Exam Code: NSE7_LED-7.0

Exam Name: Fortinet NSE 7 - LAN Edge 7.0

Version: DEMO

QUESTION 1

Refer to the exhibit. Examine the debug output shown in 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
```

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.

QUESTION 2

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.

QUESTION 3

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%

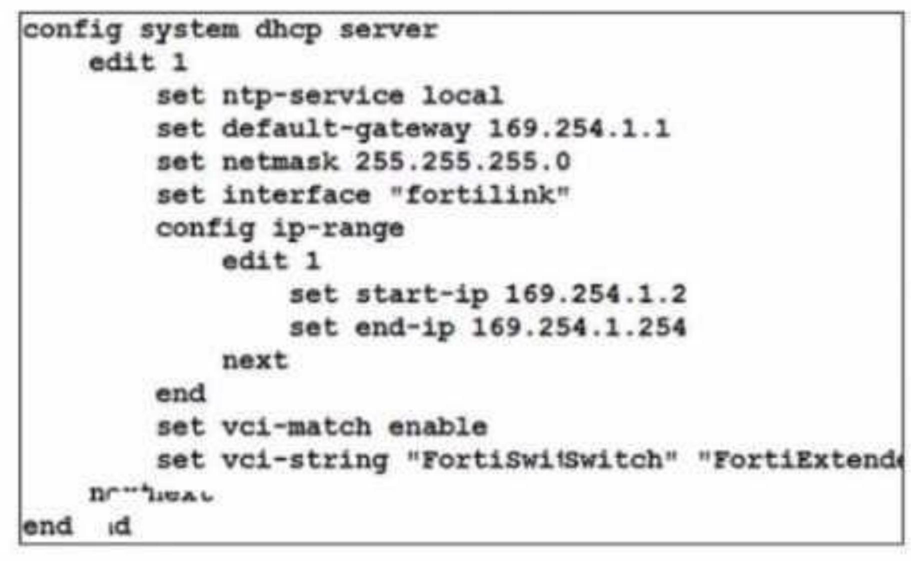
Answer: D

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.

QUESTION 4

Refer to the exhibit. By default FortiOS creates the following DHCP server scope for the FortiLink interface as shown in 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 "FortiSwiSwitch" "FortiExtend
    next
end   id
```

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.

QUESTION 5
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.

QUESTION 6

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:

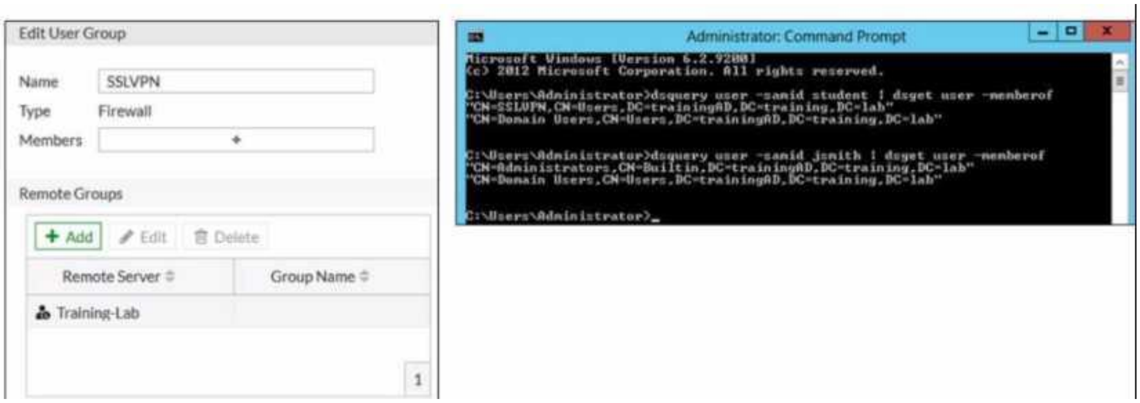
According to the FortiAuthenticator Administration Guide, "The guest portal provides pre and post-log in services for users (such as password reset and token registration abilities), and rules and replacement messages can be configured." Therefore, option C is true. The same guide also states that "Administrators 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.

QUESTION 7

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?



Edit User Group

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>_
```

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, 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.