



# Fortinet

## Exam Questions NSE7\_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

Which FortiSwitch VLANs are automatically created on FortiGate 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

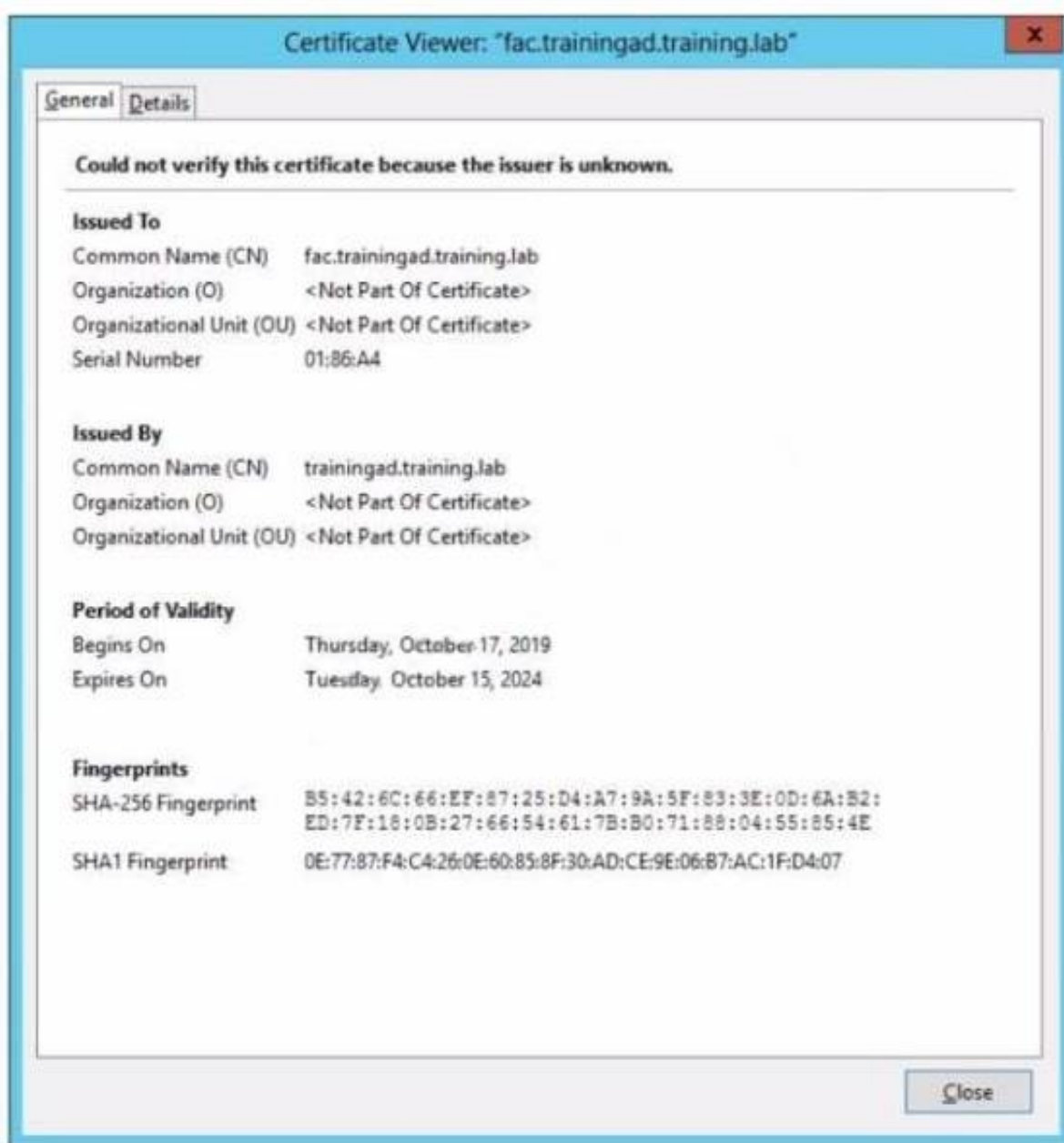
**Answer: D**

#### Explanation:

According to the FortiGate Administration Guide, "When you add a FortiSwitch device to the Security Fabric, FortiGate automatically creates the following VLANs on the FortiSwitch 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



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/#qtauthmagic=00a030293d1f411ausermac=b6:27:eb:d8a50:32aapmac=70:4c:a5:55:0d:28aapip=10.10.100.2auserip=10.0.3.1aaid=Guest03aapname=PS221STP18000148aheid=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:

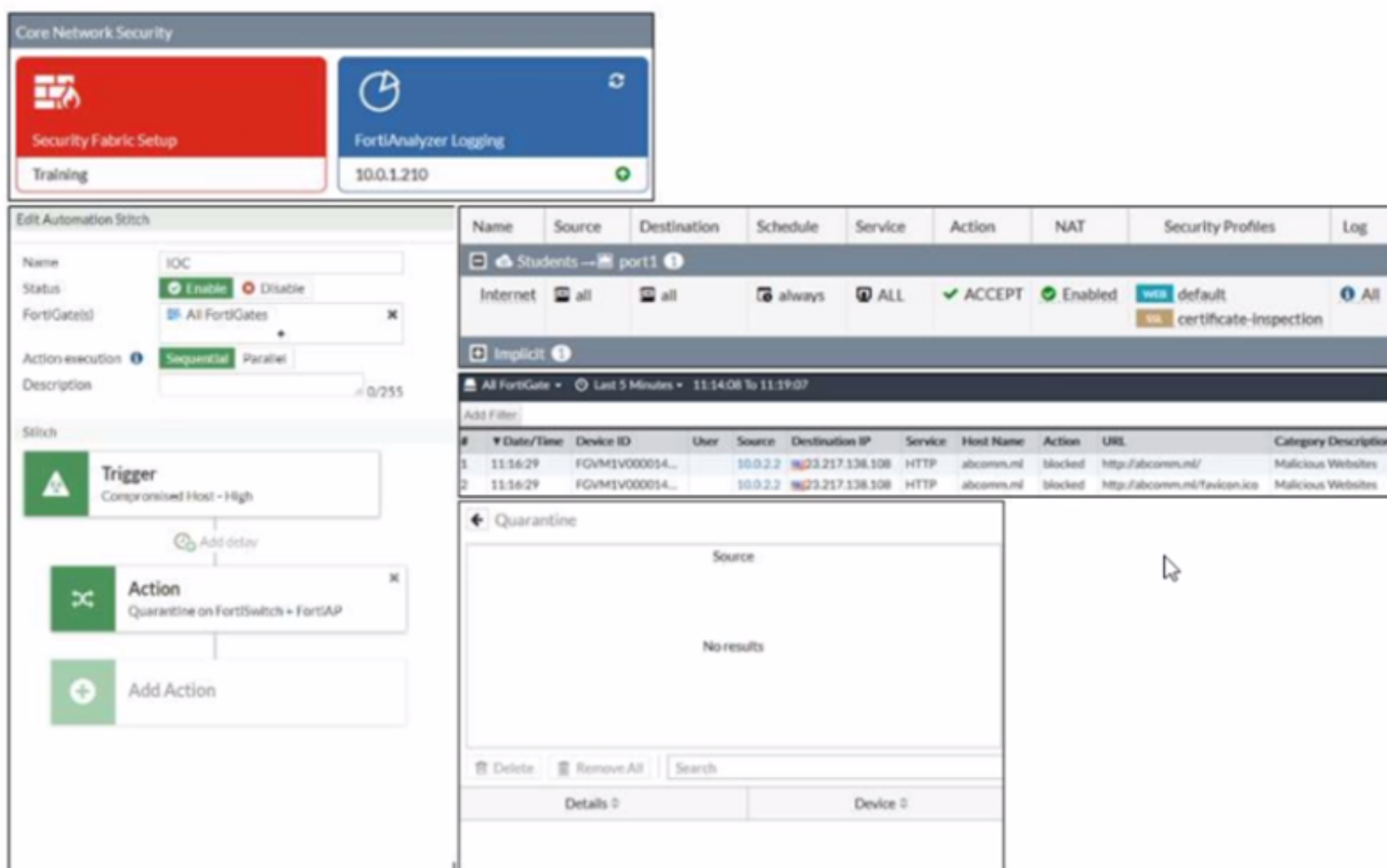
According to the FortiGate Administration Guide, “MAC address quarantine by redirect mode allows you to quarantine devices by adding their MAC addresses to a firewall address group called Quarantined Devices. The quarantined devices are kept in their current VLANs, but their traffic is redirected to 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, the 'Core Network Security' section shows 'Security Fabric Setup' with a 'Training' status and 'FortiAnalyzer Logging' with IP '10.0.1.210'. Below this, the 'Edit Automation Stitch' window is open, showing a trigger for 'Compromised Host - High' and an action for 'Quarantine on FortiSwitch + FortiAP'. To the right, the 'Log' table shows two entries for blocked HTTP requests to malicious websites. At the bottom right, the 'Quarantine' window shows 'No results'.

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

#	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	abcomm.nl	blocked	http://abcomm.nl/	Malicious Websites	
2	11:16:29	FGVM1V000014...		10.0.2.2	10.0.2.17	HTTP	abcomm.nl	blocked	http://abcomm.nl/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 (FGVM1V000014) 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

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 Guide<sup>2</sup>, “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 6

Which two statements about FortiSwitchmanager are true<sup>1</sup>? (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<sup>1</sup>, “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<sup>2</sup>, “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 anyswitch 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 7

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 8

Refer to the exhibit

```
config vpn certificate ocsf-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 ocsf-status enable
  set ocsf-option server
  set ocsf-default-server "FAC"
  set strict-ocsf-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 OCSF?

- A. Reject the student certificate if the OCSF server replies that the student certificate status is unknown
- B. Not verify the OCSF server certificate
- C. Use the OCSF URL included in the student certificate to verify the student certificate
- D. Consider the student certificate status as valid if the OCSF server is unreachable

**Answer: C**

#### Explanation:

According to the exhibit, the FortiGate configuration has ocsf-status enabled and ocsf-option set to certificate.

This means that FortiGate will use OCSF to verify the revocation status of certificates presented by

clients. According to the FortiGate Administration Guide2, "If you select certificate, FortiGate uses an OCSF 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 OCSF. Option A is false because

FortiGate will not reject the student certificate if the OCSF server replies that the student certificate status is unknown, but rather accept it as valid. Option B is

false because FortiGate will verify the OCSFserver certificate by default, unless strict-ocsf-check is disabled. Option D is false because FortiGate will not consider

the student certificate status as valid if the OCSF server is unreachable, but rather reject it as invalid.

#### NEW QUESTION 9

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" "FortiExtender"
  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

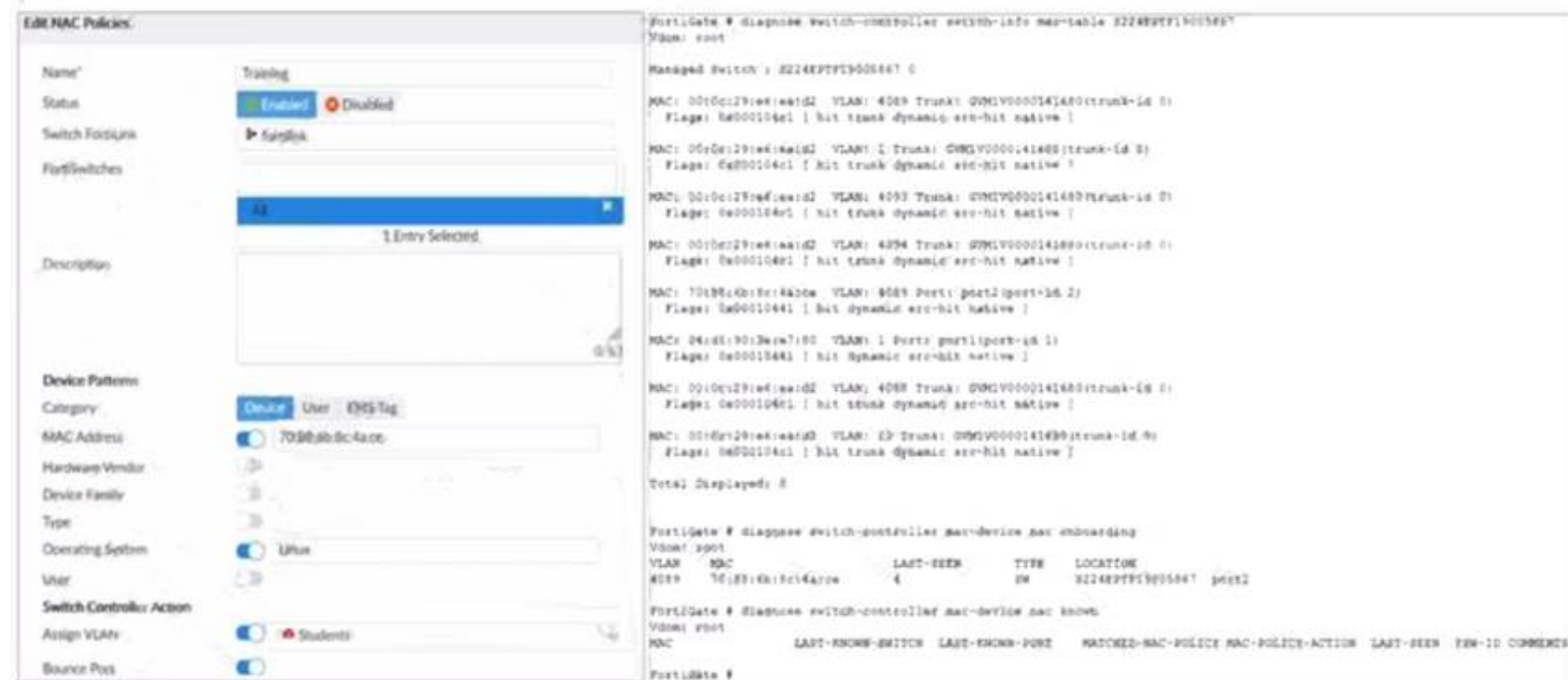
vendor device. Therefore, option C is true because the vci-string setting restricts the IP address assignment to FortiSwitch and FortiExtender devices, which use

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 10

Refer to the exhibit.



The exhibit shows the FortiManager NAC Policy configuration and the FortiGate CLI output. The NAC policy is named "Training" and is set to "Enabled". The policy is configured to match devices with the MAC address "00:0c:29:6a:2b:3c" and the operating system "Linux". The policy is applied to the "port2" interface of the "VLAN 4089" VLAN. The FortiGate CLI output shows the configuration of the "VLAN 4089" VLAN and the "port2" interface. The output also shows the MAC address of the test device as "00:0c:29:6a:2b:3d", which does not match the MAC address configured in the NAC 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 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 10

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 because FortiGate does not measure the signal strength of the weakest associated client, but rather the FortiAP does.

## NEW QUESTION 14

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 17**

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 20**

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

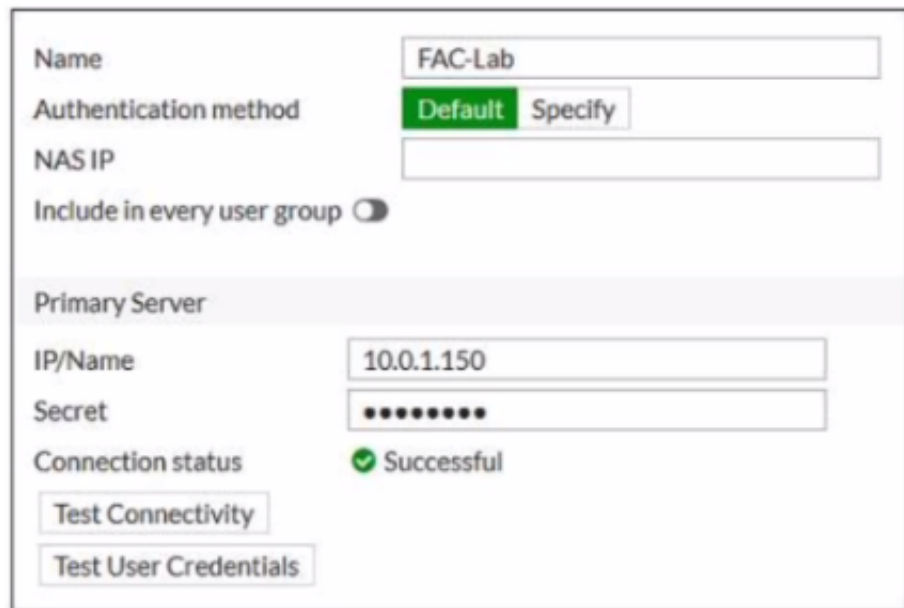
**Answer:** A

**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 25**

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 28

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 29

You are configuring a FortiGate wireless network to support automated wireless client quarantine using IOC Which two configurations must you put in place for a wireless client to be quarantined successfully? (Choose two)

- A. Configure the wireless network to be in tunnel mode
- B. Configure the FortiGate device in the Security Fabric with a FortiAnalyzer device
- C. Configure a firewall policy to allow communication
- D. Configure the wireless network to be in bridge mode

**Answer:** AB

#### Explanation:

According to the FortiGate Administration Guide, "To enable automated wireless client quarantine using IOC, you must configure the following settings: Configure your wireless network to be in tunnel mode. This allows FortiGate to inspect all wireless traffic and apply security policies. Configure your FortiGate device in the Security Fabric with a FortiAnalyzer device. This allows FortiAnalyzer to detect indicators of compromise (IOC) from wireless traffic and send quarantine commands to FortiGate." Therefore, options A and B are true because they describe the configurations that must be put in place for a wireless client to be quarantined successfully using IOC. Option C is false because configuring a firewall policy to allow communication is not required, as the default firewall policy for tunnel mode wireless networks is to allow all traffic. Option D is false because configuring the wireless network to be in bridge mode is not supported, as FortiGate cannot inspect or quarantine wireless traffic in bridge mode.

#### NEW QUESTION 34

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] fnband_pop3_start-student
[505] __fnband_cfg_get_radius_list_by_server-Loading RADIUS server 'FAC-Lab'
[342] fnband_create_radius_socket-Opened radius socket 13
[342] fnband_create_radius_socket-Opened radius socket 14
[1392] fnband_radius_auth_send-Compose RADIUS request
[1352] fnband_rad_dns_cb-10.0.1.150->10.0.1.150
[1330] __fnband_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] fnband_auth_handle_radius_result-Timer of rad 'FAC-Lab' is deleted
  800] fnband_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] fnband_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] fnband_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 36**

.....

## Relate Links

**100% Pass Your NSE7\_LED-7.0 Exam with Exambible Prep Materials**

[https://www.exambible.com/NSE7\\_LED-7.0-exam/](https://www.exambible.com/NSE7_LED-7.0-exam/)

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>