

# Fortinet

## Exam Questions NSE7\_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0



## NEW QUESTION 1

Refer to the exhibit

The exhibit shows three configuration windows in FortiGate:

- Edit External Connector:** Shows the RADIUS Single Sign-On Agent configuration. The Name is "RSSO Agent", Use RADIUS Shared Secret is checked, and Send RADIUS Responses is checked.
- Edit User Group:** Shows the RADIUS Group configuration. The Name is "RSSO Group", Type is "RADIUS Single Sign-On (RSSO)", and RADIUS Attribute Value is "Users".
- Edit Interface:** Shows the configuration for port3. Name is "port3", Type is "Physical Interface", VRF ID is "0", and Role is "Undefined". The Addressing mode is "Manual" with IP/Netmask "10.0.1.254/255.255.255.0".

Below these windows is a table showing the Firewall Policy configuration:

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Internet	port3	port1	always	ALL	ACCEPT	Enabled	no-inspection	UTM	204.09 MB
Implicit									

Examine the FortiGate RSSO configuration shown in the exhibit

FortiGate is configured to receive RADIUS accounting messages on port3 to authenticate RSSO users. The users are located behind port3 and the internet link is connected to port1. FortiGate is processing incoming RADIUS accounting messages successfully and RSSO users are getting associated with the RSSO Group user group. However, all the users are able to access the internet, and the administrator wants to restrict internet access to RSSO users only. Which configuration change should the administrator make to fix the problem?

- A. Change the RADIUS Attribute Value setting to match the name of the RADIUS attribute containing the group membership information of the RSSO users
- B. Add RSSO Group to the firewall policy
- C. Enable Security Fabric Connection on port3
- D. Create a second firewall policy from port3 to port1 and select the target destination subnets

**Answer: B**

### Explanation:

According to the exhibit, the firewall policy from port3 to port1 has no user group specified, which means that it allows all users to access the internet. Therefore, option B is true because adding RSSO Group to the firewall policy will restrict internet access to RSSO users only. Option A is false because changing the RADIUS Attribute Value setting will not affect the firewall policy, but rather the RSSO user group membership. Option C is false because enabling Security Fabric Connection on port3 will not affect the firewall policy, but rather the communication between FortiGate and other Security Fabric devices. Option D is false because creating a second firewall policy from port3 to port1 will not affect the existing firewall policy, but rather create a redundant or conflicting policy.

## NEW QUESTION 2

Which two pieces of information can the diagnose test authserver ldap command provide? (Choose two.)

- A. It displays whether the admin bind user credentials are correct
- B. It displays whether the user credentials are correct
- C. It displays the LDAP codes returned by the LDAP server
- D. It displays the LDAP groups found for the user

**Answer: BC**

### Explanation:

According to the FortiGate CLI Reference Guide, "The diagnose test authserver ldap command tests LDAP authentication with a specific LDAP server. The command displays whether the user credentials are correct and whether the user belongs to any groups that match a firewall policy. The command also displays the LDAP codes returned by the LDAP server." Therefore, options B and C are true because they describe the information that the diagnose test authserver ldap command can provide. Option A is false because the command does not display whether the admin bind user credentials are correct, but rather whether the user credentials are correct. Option D is false because the command does not display the LDAP groups found for the user, but rather whether the user belongs to any groups that match a firewall policy.

## 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 exhibits.

```
# get wireless-controller rf-analysis
WTP: Office 0-192.168.5.98:5246
```

channel	rsssi-total	rf-score	overlap-ap	interfere-ap	chan-utilizaion
1	66	8	11	11	32%
2	13	10	0	20	44%
3	6	10	0	20	16%
4	14	10	0	20	13%
5	31	10	0	20	50%
6	137	3	9	9	73%
7	32	10	0	12	58%
8	17	10	0	12	9%
9	12	10	0	14	1%
10	20	10	0	14	17%
11	79	7	3	5	32%
12	24	10	0	5	18%
13	32	10	2	5	22%

Exhibit.

```
# execute ssh 192.168.5.98
admin@192.168.5.98's password:
Office # cw_diag -c all-chutil
```

rId=0	chan=1	2412	util=82 ( 32%)
rId=0	chan=2	2417	util=113( 44%)
rId=0	chan=3	2422	util=41 ( 16%)
rId=0	chan=4	2427	util=36 ( 14%)
rId=0	chan=5	2432	util=126( 49%)
rId=0	chan=6	2437	util=165( 73%)
rId=0	chan=7	2442	util=148( 58%)
rId=0	chan=8	2447	util=26 ( 10%)
rId=0	chan=9	2452	util=5 ( 1%)
rId=0	chan=10	2457	util=46 ( 18%)
rId=0	chan=11	2462	util=82 ( 32%)
rId=0	chan=12	2467	util=45 ( 17%)
rId=0	chan=13	2472	util=50 ( 22%)

Examine the troubleshooting outputs shown in the exhibits  
 Users have been reporting issues with the speed of their wireless connection in a particular part of the wireless network The interface that is having issues is the 2 4 GHz interface that is currently configured on channel 6  
 The administrator of the wireless network has investigated and surveyed the local RF environment using the tools available at the AP and FortiGate  
 Which configuration would improve the wireless connection?

- A. Change the AP 2 4 GHz channel to 11
- B. Change the AP 2 4 GHz channel to 1.
- C. Change the AP 2 4 GHz channel to 9.
- D. Change the AP 2 4 GHz channel to 13.

**Answer: B**

#### Explanation:

According to the exhibits, the AP 2.4 GHz interface is currently configured on channel 6, which is overlapping with other nearby APs on channels 4 and 8. This can cause interference and reduce the wireless performance. Therefore, changing the AP 2.4 GHz channel to 1 would improve the wireless connection, as it would avoid the overlapping channels and use a non-overlapping channel instead. Option A is false because changing the AP 2.4 GHz channel to 11 would still overlap with other nearby APs on channels 9 and 13. Option C is false because changing the AP 2.4 GHz channel to 9 would still overlap with other nearby APs on channels 6, 8, and 11. Option D is false because changing the AP 2.4 GHz channel to 13 would still overlap with other nearby APs on channels 9 and 11.

#### NEW QUESTION 5

Which two statements about FortiSwitchmanager are true1? (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 Guide1, “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 guide2, “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 6**  
 Refer to the exhibits

SSID Profiles

Device & Groups	+ Create New Edit Clone Delete Where Used Import Column Settings				
Map View					
WiFi Templates					
AP Profile					
SSID					
WIDS Profile					
Bluetooth Profile					

<input type="checkbox"/>	Name	SSID	Traffic Mode	Security Mode	Data
<input type="checkbox"/>	SSIDs (4)				
<input type="checkbox"/>	Company Printers	Corp Printers	Tunnel	WPA2 Personal	AES
<input type="checkbox"/>	Employees-Red	employees	Tunnel	WPA2 Enterprise	AES
<input type="checkbox"/>	Guest-CorpPort	fortinet-cp	Tunnel	Captive Portal	
<input type="checkbox"/>	PSK	PSK	Tunnel	WPA2 Personal	AES

AP Profile

Name

FAPU431F-MainCampus

Comments

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 602.11ax/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 SSIDs 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 7**

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 8**

An administrator has configured an SSID in bridge mode for corporate employees All APs are online and provisioned using default AP profiles Employees are unable to locate the SSID to conned  
Which two configurations can the administrator verify? (Choose two)

- A. Verify that the broadcast SSID option is enabled in the SSID configuration
- B. Verify that the Block Intra-SSID Traffic (intra-vap-privacy) option in the SSID configuration is disabled
- C. Verify that the SSID to an AP group that should be broadcasting the SSID is applied
- D. Verify that the SSID is manually applied on AP profiles for both 2 4 GHz and 5 GHz radios

**Answer:** AC

**Explanation:**

According to the FortiAP Configuration 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. You must also enable Broadcast SSID." Therefore, option A is true because the broadcast SSID option allows the SSID to be visible to wireless clients. Option C is also true because the SSID must be applied to an AP group that contains the APs that should be broadcasting the SSID. According to the same guide1, "You can create AP groups and assign them to different locations or departments. You can then apply different settings, such as SSIDs, to each group." Option B is false because blocking intra-SSID traffic prevents wireless clients on the same SSID from communicating with each other, which is not related to broadcasting the SSID. Option D is false because the SSID can be applied to an AP group or a global profile, which will automatically apply to all APs, without manually configuring each AP profile.

**NEW QUESTION 9**

Refer to the exhibit

```
config vpn certificate ocap-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 ocap-status enable
  set ocap-option server
  set ocap-default-server "FAC"
  set strict-ocap-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 OCAP?

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

**Answer:** C

**Explanation:**

According to the exhibit, the FortiGate configuration has ocap-status enabled and ocap-option set to certificate. This means that FortiGate will use OCAP to verify the revocation status of certificates presented by clients. According to the FortiGate Administration Guide2, "If you select certificate, FortiGate uses an OCAP 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 OCAP. Option A is false because FortiGate will not reject the student certificate if the OCAP server replies that the student certificate status is unknown, but rather accept it as valid. Option B is

false because FortiGate will verify the OCSPserver certificate by default, unless strict-ocsp-check is disabled. Option D is false because FortiGate will not consider the student certificate status as valid if the OCSP server is unreachable, but rather reject it as invalid.

#### NEW QUESTION 10

Refer to the exhibits.

Firewall Policy

```
config firewall policy
  edit 11
    set name "Guest to Internal"
    set uuid c5e45130-aada-51e8-ee0c-bc1204f9f163
    set srcintf "guest"
    set dstintf "port3"
    set srcaddr "all"
    set dstaddr "FortiAuthenticator" "WindowsAD"
    set action accept
    set schedule "always"
    set service "ALL"
  next
end
```

Examine the firewall policy configuration and SSID settings

An administrator has configured a guest wireless network on FortiGate using the external captive portal. The administrator has verified that the external captive portal URL is correct. However, wireless users are not able to see the captive portal login page.

Given the configuration shown in the exhibit and the SSID settings, which configuration change should the administrator make to fix the problem?

- A. Disable the user group from the SSID configuration
- B. Enable the captive-portal-exempt option in the firewall policy with the ID 11.
- C. Apply a guest.portal user group in the firewall policy with the ID 11.
- D. Include the wireless client subnet range in the Exempt Source section

**Answer: C**

#### Explanation:

According to the FortiGate Administration Guide, "To use an external captive portal, you must configure a user group that uses the external captive portal as the authentication method and apply it to a firewall policy." Therefore, option C is true because it will allow the wireless users to be redirected to the external captive portal URL when they try to access the Internet. Option A is false because disabling the user group from the SSID configuration will prevent the wireless users from being authenticated by the FortiGate device. Option B is false because enabling the captive-portal-exempt option in the firewall policy will bypass the captive portal authentication for the wireless users, which is not the desired outcome. Option D is false because including the wireless client subnet range in the Exempt Source section will also bypass the captive portal authentication for the wireless users, which is not the desired outcome.

#### 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 15**  
 Exhibit.

**Network Topology**

Internet (port1) connects to FortiGate (port1). FortiGate (port3) connects to FortiAuthenticator (10.0.1.150) and WindowsAD (10.0.1.10). FortiGate (port4) connects to a wireless AP (10.0.13.254/24). The SSID 'Guest' has Subnet 10.0.20.0/24 and DNS 10.0.1.10.

**WiFi Settings**  
 SSID: Guest

Client link: ☒   
 Broadcast SSID: ☒

**Security Mode Settings**  
 Security mode: Captive Portal   
 Portal type: Authentication   
 Authentication portal: Local   
 External URL: https://fac.traininglab.com/guest

**User groups**  
 guest.portal

**Exempt sources**  
 FortiAuthenticator   
 WindowsAD

**Exempt destinations/services**  
 Redirect after Captive Portal: Original Request

**Client MAC Address Filtering**  
 MAC address filtering: ☒

**Additional Settings**  
 Schedule: always   
 Block intra-SSID traffic: ☒   
 Optional VLAN ID: 0   
 Broadcast suppression: ☒   
 ARP for known clients: ☒   
 DHCP uplink: ☒

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Guest01 (Guest-Access) → port1										
12	guest internet access	all	all	always	ALL	ACCEPT	Enabled		UTM	0B
Guest01 (Guest-Access) → port3										
13	Internal	all	FortiAuthenticator WindowsAD	always	ALL	ACCEPT	Disabled		UTM	0B

Refer to the exhibit showing a network topology and SSID settings. FortiGate is configured to use an external captive portal. However, wireless users are not able to see the captive portal login page. Which configuration change should the administrator make to fix the problem?

- A. Enable NAT in the firewall policy with the ID 13.
- B. Add the FortiAuthenticator and WindowsAD address objects as exempt destinations services
- C. Enable the captive-portal-exempt option in the firewall policy with the ID 12
- D. Remove the guest.portal user group in the firewall policy with the ID 12

**Answer: B**

**Explanation:**

According to the exhibit, the network topology and SSID settings show that FortiGate is configured to use an external captive portal hosted on FortiAuthenticator, which is connected to a Windows AD server for user authentication. However, wireless users are not able to see the captive portal login page, which means that they are not redirected to the external captive portal URL. Therefore, option B is true because adding the FortiAuthenticator and WindowsAD address objects as exempt destinations services will allow the wireless users to access the external captive portal URL without being blocked by the firewall policy. Option A is false because enabling NAT in the firewall policy with the ID 13 will not affect the redirection to the external captive portal URL, but rather the source IP address of the wireless traffic. Option C is false because enabling the captive-portal-exempt option in the firewall policy with the ID 12 will bypass the captive portal authentication for the wireless users, which is not the desired outcome. Option D is false because removing the guest.portal user group in the firewall policy with the ID 12 will prevent the wireless users from being authenticated by FortiGate, which is required for accessing the external captive portal.

**NEW QUESTION 18**  
 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

Test Connectivity

Test User Credentials



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 `diagnose test 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 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 2, "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 23**

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 26**

.....



## 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](#)**