

# Fortinet

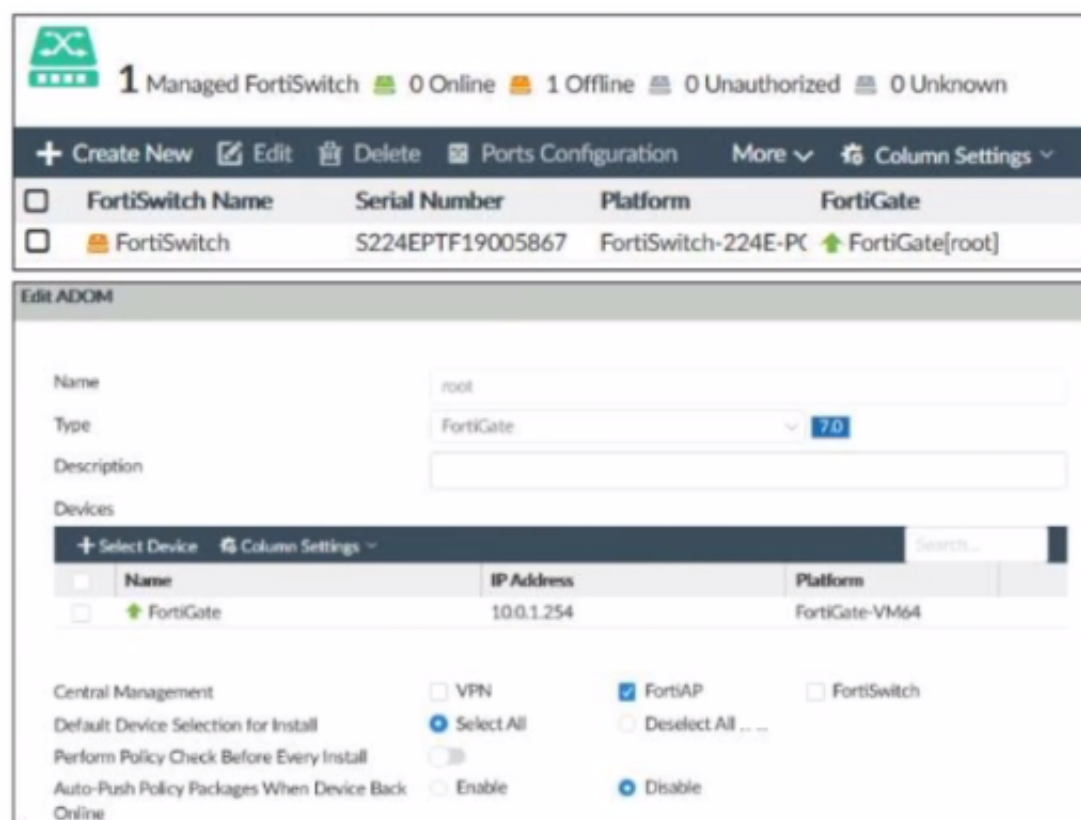
## Exam Questions NSE7\_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0



## NEW QUESTION 1

Refer to the exhibit.



Examine the FortiManager information shown in the exhibit

Which two statements about the FortiManager status are true" (Choose two)

- A. FortiSwitch manager is working in per-device management mode
- B. FortiSwitch is not authorized
- C. FortiSwitch manager is working in central management mode
- D. FortiSwitch is authorized and offline

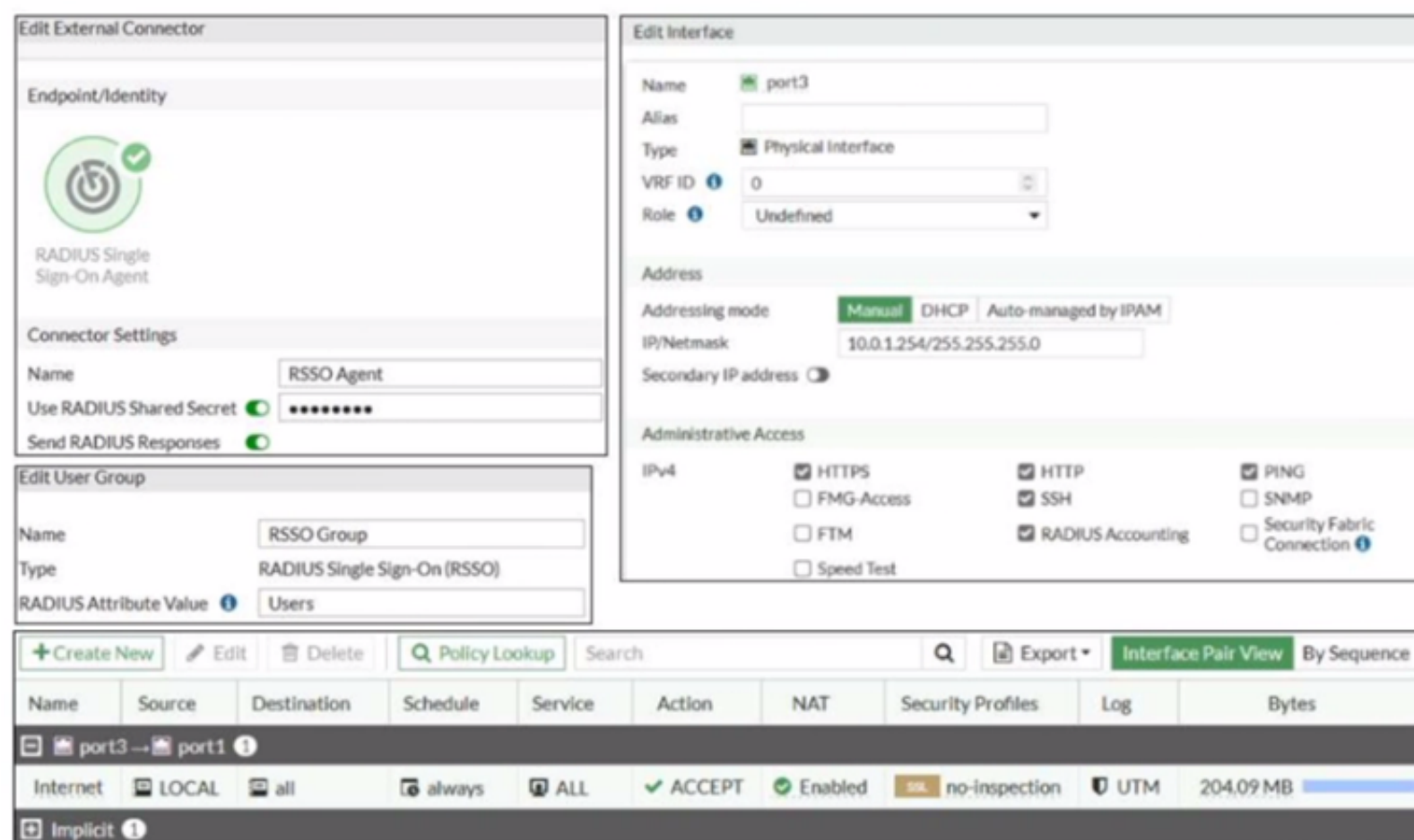
**Answer: CD**

### Explanation:

According to the FortiManager Administration Guide, "Central management mode allows you to manage all FortiSwitch devices from a single interface on the FortiManager device." Therefore, option C is true because the exhibit shows that the FortiSwitch manager is enabled and the FortiSwitch device is managed by the FortiManager device. Option D is also true because the exhibit shows that the FortiSwitch device status is offline, which means that it is not reachable by the FortiManager device, but it is authorized, which means that it has been added to the FortiManager device. Option A is false because per-device management mode allows you to manage each FortiSwitch device individually from its own web-based manager or CLI, which is not the case in the exhibit. Option B is false because the FortiSwitch device is authorized, as explained above.

## NEW QUESTION 2

Refer to the exhibit



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 selling 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 lo 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 3**

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 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**

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

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

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

**Answer:** D

**Explanation:**

According to the FortiAP Configuration Guide, "Channel utilization measures how busy a channel is over a given period of time. It includes both Wi-Fi and non-Wi-Fi interference sources. A high channel utilization indicates a congested channel and can result in poor wireless performance. The recommended maximum utilization value that an interface should not exceed is 65%." Therefore, option D is true because it gives the recommended maximum utilization value for an interface in the 5 GHz range. Options A, B, and C are false because they give higher utilization values that can cause poor wireless performance.

<https://docs.fortinet.com/document/fortiap/7.0.0/configuration-guide/734537/wireless-radio-settings#channel-uti>

**NEW QUESTION 6**

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 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

Refer to the exhibit.

EDR NAC Policies

Name

Trailing

Status

Enabled

Disabled

Switch Port/Ports

4089

FortiSwitches

AS

Description

1 Entry Selected

Device Patterns

Category

Device

User

EMS-Tag

MAC Address

70984b3c4a3e

Hardware Vendor

HP

Device Family

HP

Type

HP

Operating System

Linux

User

HP

Switch Controller Action

Assign VLAN

Students

Source Port

port2

FortiGate # diagnose switch-controller switch-info mac-table S224EPTF1905547

Vlan: port2

Managed Switch: S224EPTF1905547 0

MAC: 00:0c:29:6a:2b:3d VLAN: 4089 Trunk: 0001V0000141680(trunk-id 0)

Flags: 0a000104e1 | hit trunk dynamic src-hit native |

MAC: 00:0c:29:6a:2b:3d VLAN: 1 Trunk: 0001V0000141680(trunk-id 0)

Flags: 0a000104e1 | hit trunk dynamic src-hit native |

MAC: 00:0c:29:6a:2b:3d VLAN: 4089 Trunk: 0001V0000141680(trunk-id 0)

Flags: 0a000104e1 | hit trunk dynamic src-hit native |

MAC: 00:0c:29:6a:2b:3d VLAN: 4089 Trunk: 0001V0000141680(trunk-id 0)

Flags: 0a000104e1 | hit trunk dynamic src-hit native |

MAC: 70984b3c4a3e VLAN: 9089 Ports: port2(post-id 1)

Flags: 0a000104e1 | hit dynamic src-hit native |

MAC: 04:0d:90:3a:71:00 VLAN: 1 Ports: port1(post-id 1)

Flags: 0a000104e1 | hit dynamic src-hit native |

MAC: 00:0c:29:6a:2b:3d VLAN: 4089 Trunk: 0001V0000141680(trunk-id 0)

Flags: 0a000104e1 | hit trunk dynamic src-hit native |

MAC: 00:0c:29:6a:2b:3d VLAN: 1 Trunk: 0001V0000141680(trunk-id 0)

Flags: 0a000104e1 | hit trunk dynamic src-hit native |

Total Displayed: 8

FortiGate # diagnose switch-controller mac-device mac onboarding

Vlan: port2

MAC RAC LAST-SEEN TYPE LOCATION

4089 70984b3c4a3e 4 SW S224EPTF1905547 port2

FortiGate # diagnose switch-controller mac-device mac known

Vlan: port2

MAC LAST-KNOWN-SWITCH LAST-KNOWN-PORT MATCHED-MAC-POLICY MAC-POLICY-ACTION LAST-SEEN TEN-ID COMMENTS

FortiGate #

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 9

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 Guide, "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 10**

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 12**

Exhibit.

**Network Topology**

Internet --- port1 (10.0.13.254/24) --- port2 (10.0.1.254/24) --- FortiAuthenticator (10.0.1.150) --- WindowsAD (10.0.1.10)

SSID: Guest  
 Subnet: 10.0.20.0/24  
 DNS: 10.0.1.10

**SSID Settings**

SSID: Guest

Client limit: ☐ Broadcast SSID: ☒

**Security Mode Settings**

Security mode: Captive Portal  
 Portal type: Authentication  
 Authentication portal: Local **External**  
 URL: https://far.trainingall.training.fab/guest

**User groups**

- guest.portal

**Exempt sources**

- FortiAuthenticator
- WindowsAD

**Exempt destinations/services**

- Original Request
- Specific URL

**Client MAC Address Filtering**

MAC address filtering: ☐

**Additional Settings**

Schedule: always

Block intra-SSID traffic: ☒

Optional VLAN ID: 0

Broadcast suppression: ☒

**Firewall Policy Table**

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) --> port2										
13	internal	all	FortiAuthenticator	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 16**

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

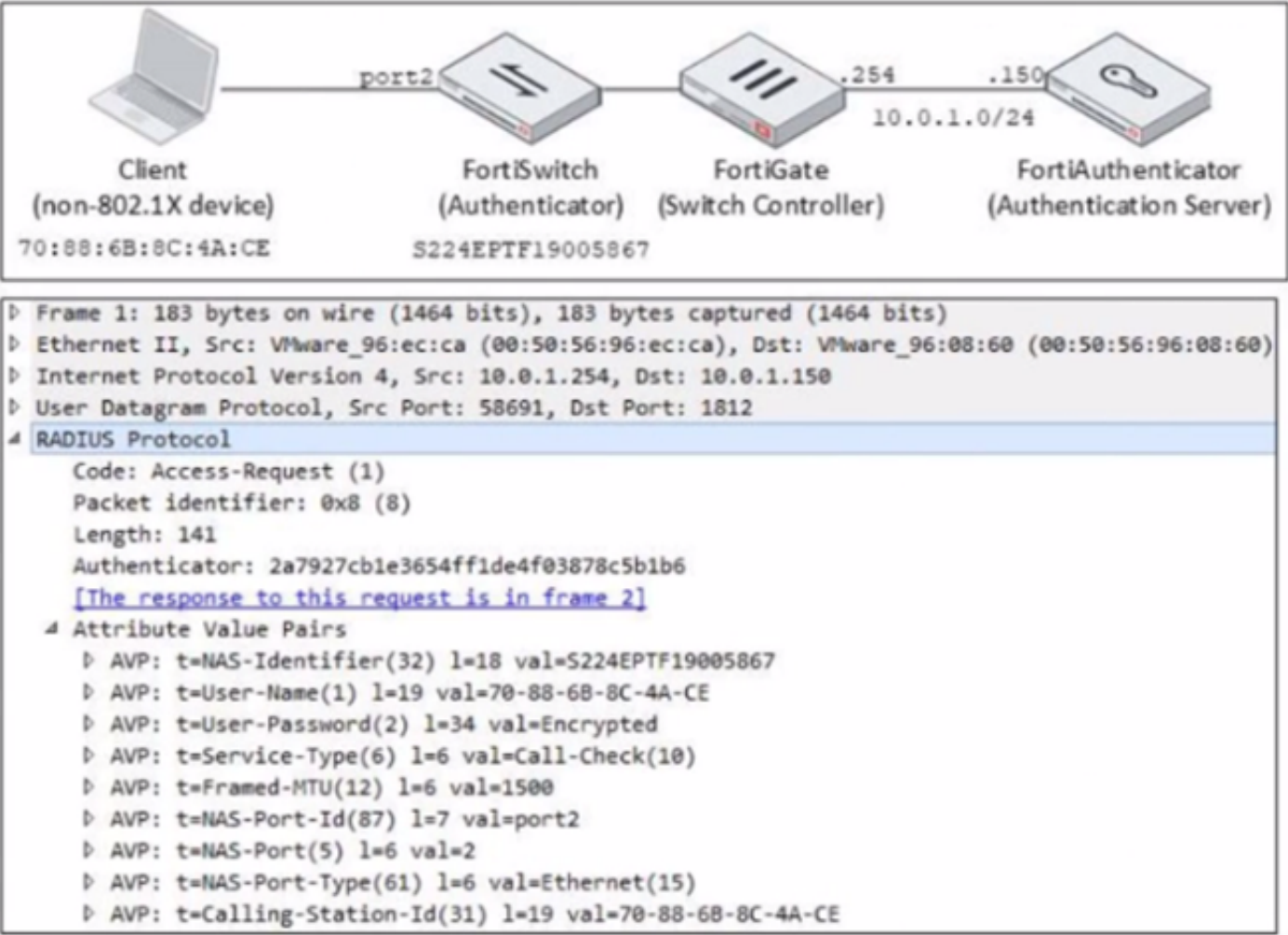
**Answer:** BD

**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 20**

Refer to the exhibit.



Examine the network diagram and packet capture shown in the exhibit  
 The packet capture was taken between FortiGate and FortiAuthenticator and shows a RADIUS Access-Request packet sent by FortiSwitch to FortiAuthenticator through FortiGate  
 Why does the User-Name attribute in the RADIUS Access-Request packet contain the client MAC address?

- A. The client is performing AD machine authentication
- B. FortiSwitch is authenticating the client using MAC authentication bypass
- C. The client is performing user authentication
- D. FortiSwitch is sending a RADIUS accounting message to FortiAuthenticator

**Answer:** B

**Explanation:**

According to the exhibit, the User-Name attribute in the RADIUS Access-Request packet contains the client MAC address of 00:0c:29:6a:2b:3d. This indicates that FortiSwitch is authenticating the client using MAC authentication bypass (MAB), which is a method of authenticating devices that do not support 802.1X by using their MAC address as the username and password. Therefore, option B is true because it explains why the User-Name attribute contains the client MAC address. Option A is false because AD machine authentication uses a computer account name and password, not a MAC address. Option C is false because user authentication uses a user name and password, not a MAC address. Option D is false because FortiSwitch is sending a RADIUS Access-Request message to FortiAuthenticator, not a RADIUS accounting message.

**NEW QUESTION 25**

Refer to the exhibit.



**Edit VPN Tunnel**

Name: IPsec-VPN

Comments:

---

**Network** Edit

Remote Gateway : Dialup User , Interface : port2

IPv4 client address range : 10.0.1.15-10.0.1.50/255.255.255.255

IPv6 client address range : ::-::/128

---

**Authentication** ✓ ↺

Method:

Pre-shared Key:

**IKE**

Version:

Mode: ☒ Aggressive ☐ Main (ID protection)

Peer Options

Accept Types:

---

**Phase 1 Proposal** Edit

Algorithms : AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1, 3DES-SHA256

Diffie-Hellman Groups : 14, 5

---

**XAUTH** Edit

Type : Disabled

Examine the IPsec VPN phase 1 configuration shown in the exhibit

An administrator wants to use certificate-based authentication for an IPsec VPN user

Which three configuration changes must you make on FortiGate to perform certificate-based authentication for the IPsec VPN user? (Choose three)

- A. Create a PKI user for the IPsec VPN user, and then configure the IPsec VPN tunnel to accept the PKI user as peer certificate
- B. In the Authentication section of the IPsec VPN tunnel in the Method drop-down list select Signature and then select the certificate that FortiGate will use for IPsec VPN
- C. In the IKE section of the IPsec VPN tunnel in the Mode field select Main (ID protection)
- D. Import the CA that signed the user certificate
- E. Enable XAUTH on the IPsec VPN tunnel

**Answer: BDE**

**Explanation:**

According to the FortiGate Administration Guide, "To use certificate-based authentication, you must configure the following settings on both peers: Select Signature as the authentication method and select a certificate to use for authentication. Import the CA certificate that issued the peer's certificate. Enable XAUTH on the phase 1 configuration." Therefore, options B, D, and E are true because they describe the configuration changes that must be made on FortiGate to perform certificate-based authentication for the IPsec VPN user. Option A is false because creating a PKI user for the IPsec VPN user is not required, as the user certificate can be verified by the CA certificate. Option C is false because changing the IKE mode to Main (ID protection) is not required, as the IKE mode can be either Main or Aggressive for certificate-based authentication.

**NEW QUESTION 26**

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 31**

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 user="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 secs 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 35**

.....

## 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](#)**