

Fortinet

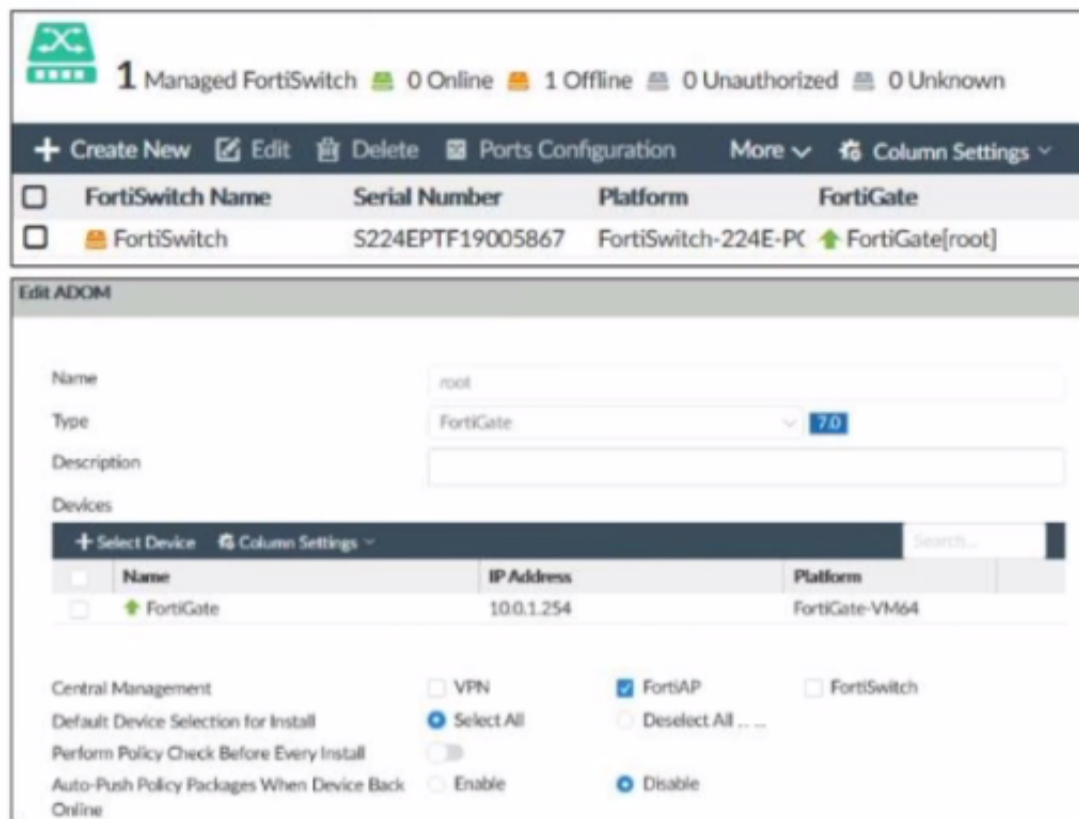
Exam Questions NSE7_LED-7.0

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

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 3

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 4

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 5

Refer to the exhibit.

The screenshot displays the FortiManager configuration interface on the left and FortiGate CLI output on the right. The configuration shows a NAC policy named 'Training' with status 'Enabled', assigned to 'port2' on 'FortiSwitch1'. The policy is configured with 'Device Patterns' including 'Desktop', 'User', and 'EWS-Tag'. The 'MAC Address' field is set to '70:8b:ab:3c:4a:0e'. The 'Operating System' is set to 'Linux'. The 'Switch Controller Action' is set to 'Assign VLAN' with 'Assign VLAN' set to 'Students'. The 'Source Port' is set to 'port2'. The CLI output on the right shows the 'diagnose switch-controller mac-info map-table' command output, which lists MAC addresses and their associated VLANs. The 'diagnose switch-controller mac-device mac onboarding' command output shows a table with columns: VLAN, MAC, LAST-SEEN, TYPE, LOCATION. The table shows a device with MAC '70:8b:ab:3c:4a:0e' on VLAN '4089' at location 'port2'.

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 m 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 6

An administrator is testing the connectivity for a new VLAN The devices in the VLAN are connected to a FortiSwitch device that is managed by FortiGate Quarantine is disabled on FortiGate While testing the administrator noticed that devices can ping FortiGate and FortiGate can ping the devices The administrator also noticed that inter-VLAN communication works However intra-VLAN communication does not work Which scenario is likely to cause this issue?

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

Answer: C

Explanation:

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

NEW QUESTION 7

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 8

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

NEW QUESTION 9

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

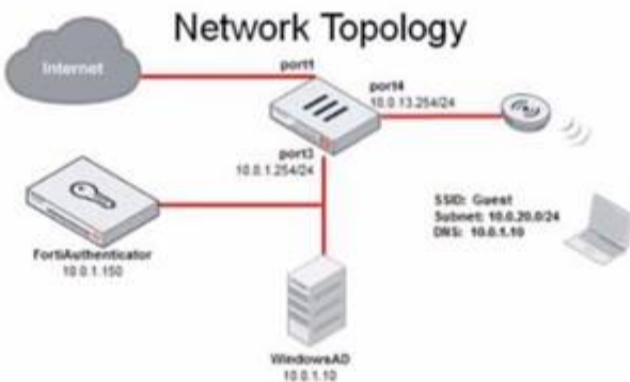
Explanation:

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 10

Exhibit.

Network Topology



The diagram shows a network topology. An Internet cloud is connected to a FortiGate (port1, 10.0.13.254/24). The FortiGate is also connected to a FortiAuthenticator (10.0.1.150) and a WindowsAD server (10.0.1.10). The FortiGate has two other ports: port14 (10.0.13.254/24) and port13 (10.0.1.254/24). A wireless client is connected to port14. The SSID is 'Guest' with Subnet 10.0.20.0/24 and DNS 10.0.1.10.

WiFi Settings

SSID: Guest

Client limit: 0

Broadcast SSID: ☒

Security Mode Settings

Security mode: Captive Portal

Portal type: Authentication

Authentication portal: Local **External**

Authentication portal URL: https://far.trainingsoft.org/portal/guest

User groups: guest.portal

Exempt sources: FortiAuthenticator, WindowsAD

Exempt destinations/services:

Redirect after Captive Portal: Original Request, Specific URL

Client 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) → port13										
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

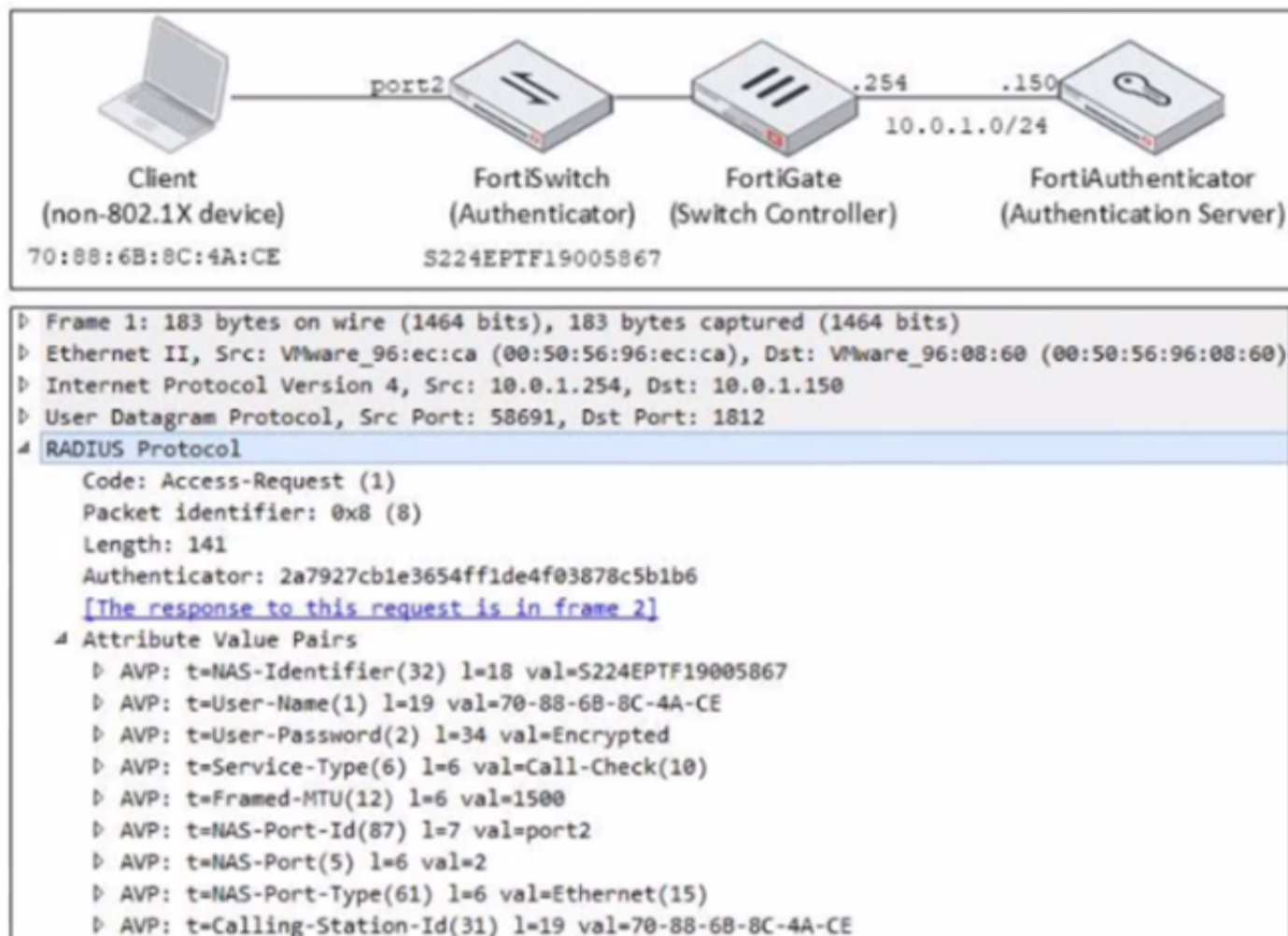
Explanation:

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 10

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

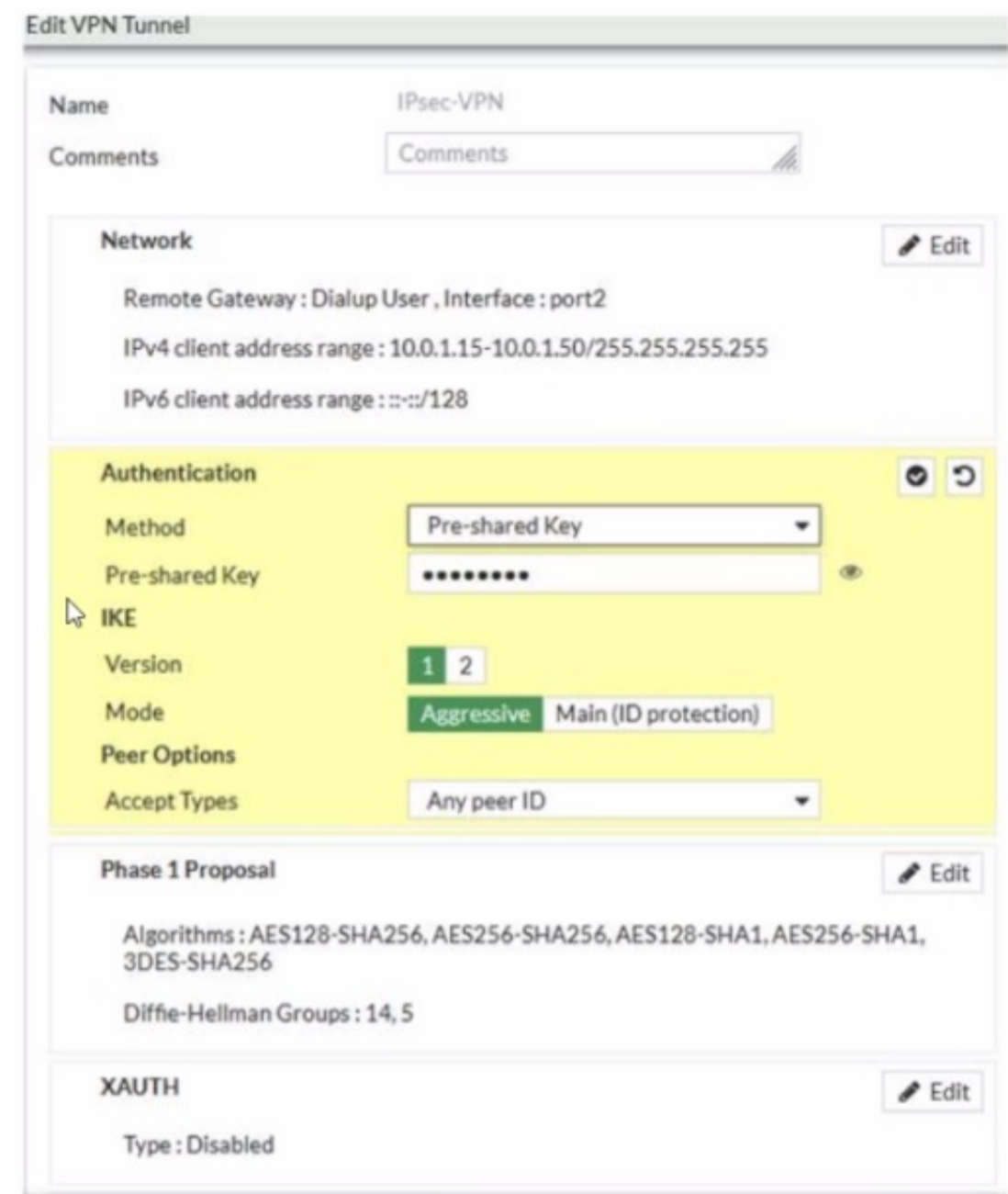
Answer: B

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 13

Refer to the exhibit.



The screenshot shows the 'Edit VPN Tunnel' configuration page for an IPsec-VPN. The 'Name' field is 'IPsec-VPN'. The 'Comments' field is empty. The 'Network' section shows 'Remote Gateway : Dialup User , Interface : port2', 'IPv4 client address range : 10.0.1.15-10.0.1.50/255.255.255.255', and 'IPv6 client address range : :::/128'. The 'Authentication' section is highlighted in yellow and shows 'Method' set to 'Pre-shared Key', 'Pre-shared Key' field with masked characters, and 'IKE' section with 'Version' set to 1, 'Mode' set to 'Aggressive', and 'Accept Types' set to 'Any peer ID'. The 'Phase 1 Proposal' section shows 'Algorithms : AES128-SHA256, AES256-SHA256, AES128-SHA1, AES256-SHA1, 3DES-SHA256' and 'Diffie-Hellman Groups : 14, 5'. The 'XAUTH' section shows '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

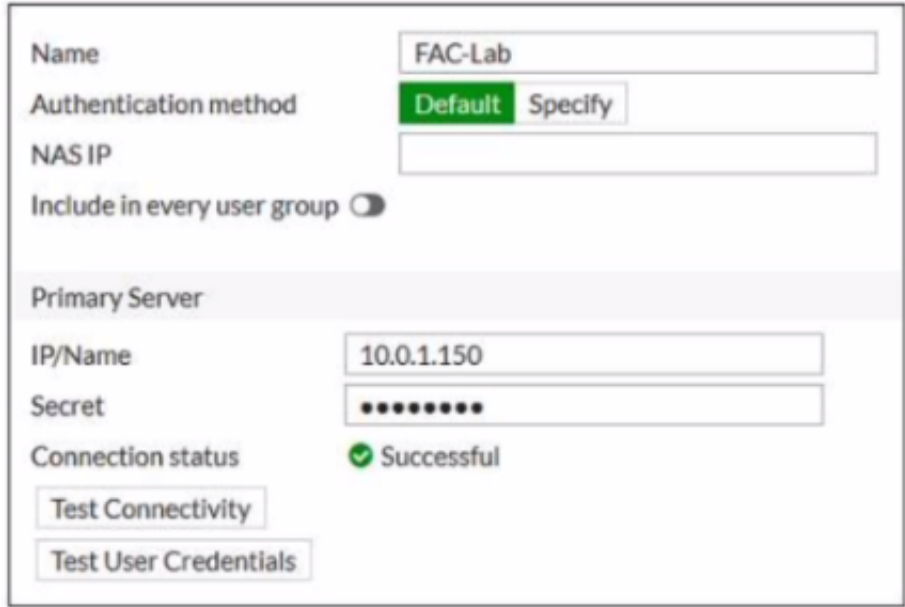
Answer: BDE

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 15

Refer to the exhibit.



The screenshot shows the 'RADIUS server' configuration page. The 'Name' field is 'FAC-Lab'. The 'Authentication method' is set to 'Default'. The 'NAS IP' field is empty. The 'Include in every user group' checkbox is unchecked. The 'Primary Server' section shows 'IP/Name' set to '10.0.1.150', 'Secret' field with masked characters, and 'Connection status' set to 'Successful'. There are buttons for 'Test Connectivity' and '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 `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 20

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=00000001d 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 21

.....

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](#)