Number: NSE7_LED-7.0
Passing Score: 800
Time Limit: 120 min
File Version: 5.0

Exam Code: NSE7_LED-7.0

Exam Name: Fortinet NSE 7 - LAN Edge 7.0

Exam A

QUESTION 1
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

Correct Answer: B, C
Section:
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.

QUESTION 2
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

Correct Answer: A, D, E
Section:
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.

QUESTION 3
Refer to the exhibit.

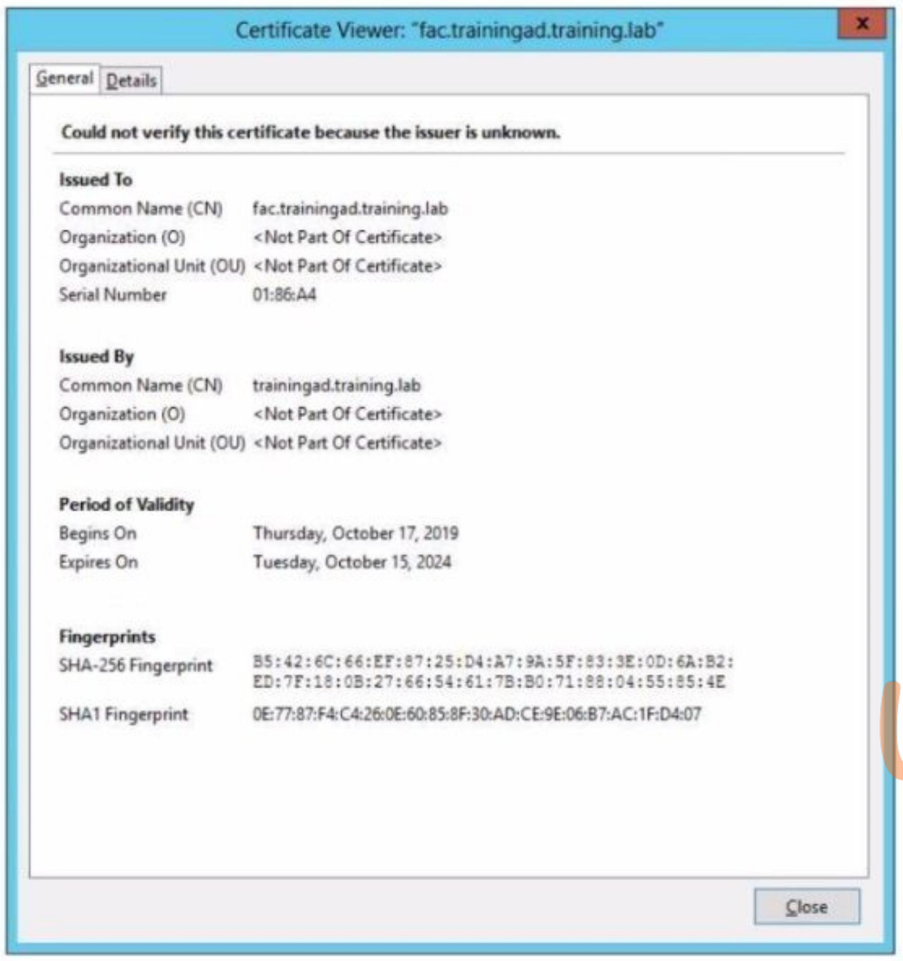
```
config system dhcp server
    edit 1
        set ntp-service local
        set default-gateway 169.254.1.1
        set netmask 255.255.255.0
        set interface "fortilink"
        config ip-range
            edit 1
                set start-ip 169.254.1.2
                set end-ip 169.254.1.254
            next
        end
        set vci-match enable
        set vci-string "FortiSwitch" "FortiExtende
    next
end
```

By default FortiOS creates the following DHCP server scope for the FortiLink interface as shown in the exhibit
What is the objective of the vci-string setting?

A. To ignore DHCP requests coming from FortiSwitch and FortiExtender devices
B. To reserve IP addresses for FortiSwitch and FortiExtender devices
C. To restrict the IP address assignment to FortiSwitch and FortiExtender devices
D. To restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname

Correct Answer: C
Section:
Explanation:
According to the exhibit, the DHCP server scope for the FortiLink interface has a vci-string setting with the value "Cisco AP c2700". This setting is used to match the vendor class identifier (VCI) of the DHCP clients that request an IP address from the DHCP server. The VCI is a text string that uniquely identifies a type of vendor device. Therefore, option C is true because the vci-string setting restricts the IP address assignment to FortiSwitch and FortiExtender devices, which use the VCI "Cisco AP c2700". Option A is false because the vci-string setting does not ignore DHCP requests coming from FortiSwitch and FortiExtender devices, but rather accepts them. Option B is false because the vci-string setting does not reserve IP addresses for FortiSwitch and FortiExtender devices, but rather assigns them dynamically. Option D is false because the vci-string setting does not restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname, but rather to devices that have "Cisco AP c2700" as their VCI.

QUESTION 4
Refer to the exhibit.



Wireless guest users are unable to authenticate because they are getting a certificate error while loading the captive portal login page. This URL string is the HTTPS POST URL guest wireless users see when attempting to access the network using the web browser

```
https://fac.trainingad.training.com/guests/login/?
login&post=https://auth.trainingad.training.lab:1003/fgtauth&magic=000a038293d1f411&usermac=b8:27:eb:d8:50:02&apmac=70:4c:a5:9d:0d:28&apip=10.10.100.2&userip=10.0.3.1&ssid=Guest03&apname=PS221ETF18000148&bssid=70:4c:a5:
```

Which two settings are the likely causes of the issue? (Choose two.)

A. The external server FQDN is incorrect
B. The wireless user's browser is missing a CA certificate
C. The FortiGate authentication interface address is using HTTPS
D. The user address is not in DDNS form

Correct Answer: A, B
Section:
Explanation:
According to the exhibit, the wireless guest users are getting a certificate error while loading the captive portal login page. This means that the browser cannot verify the identity of the server that is hosting the login

page. Therefore, option A is true because the external server FQDN is incorrect, which means that it does not match the common name or subject alternative name of the server certificate. Option B is also true because the wireless user's browser is missing a CA certificate, which means that it does not have the root or intermediate certificate that issued the server certificate. Option C is false because the FortiGate authentication interface address is using HTTPS, which is a secure protocol that encrypts the communication between the browser and the server. Option D is false because the user address is not in DDNS form, which is not related to the certificate error.

QUESTION 5
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

Correct Answer: A
Section:
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.

QUESTION 6
Refer to the exhibit

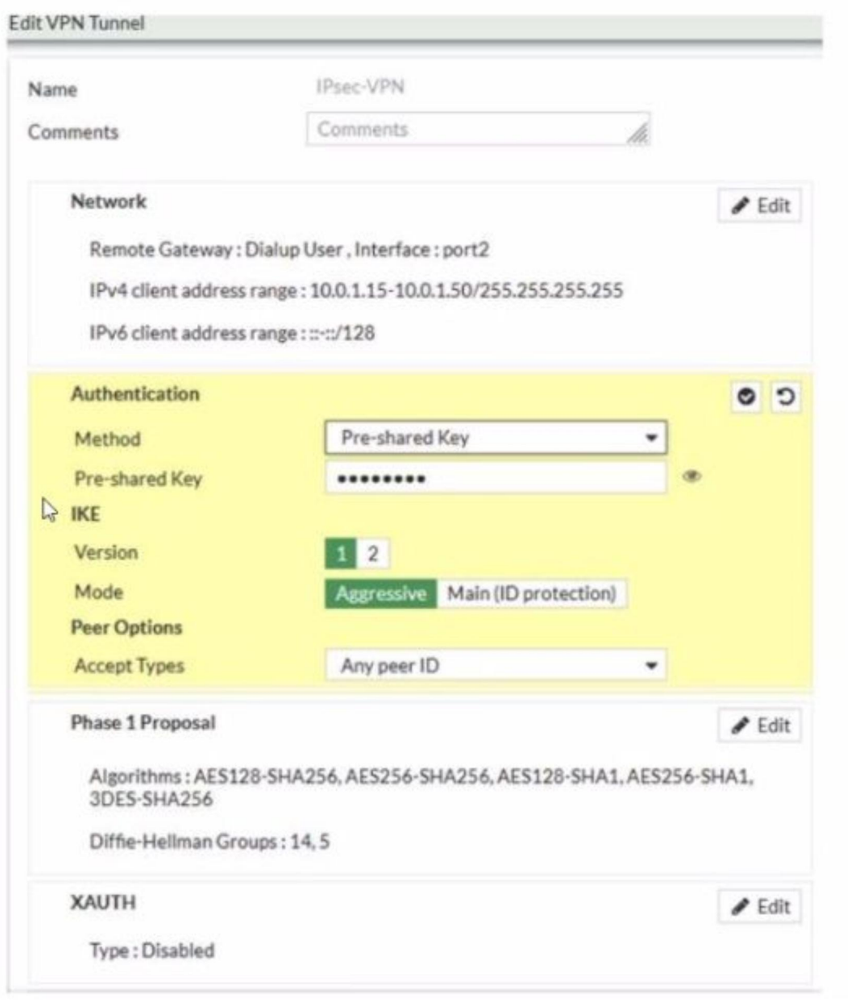
```
config vpn certificate ocsp-server
    edit "FAC"
        set url "http://10.0.1.150:2560"
        set cert "CA_Cert_1"
        set unavail-action revoke
    next
end
config vpn certificate setting
    set ocsp-status enable
    set ocsp-option server
    set ocsp-default-server "FAC"
    set strict-ocsp-check 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 OCSP?
A. Reject the student certificate if the OCSP server replies that the student certificate status is unknown
B. Not verify the OCSP server certificate
C. Use the OCSP URL included in the student certificate to verify the student certificate
D. Consider the student certificate status as valid if the OCSP server is unreachable

Correct Answer: C
Section:
Explanation:

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

QUESTION 7
Refer to the exhibit.



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

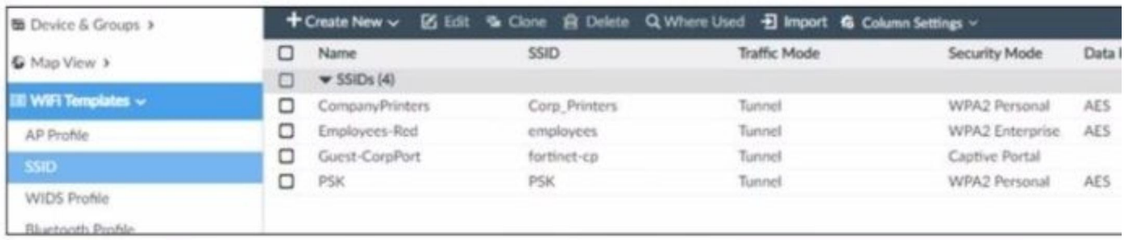
Correct Answer: B, D, E
Section:
Explanation:
According to the FortiGate Administration Guide, "To use certificate-based authentication, you must configure the following settings on both peers: Select Signature as the authentication method and select a certificate to use for authentication. Import the 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.

QUESTION 8
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

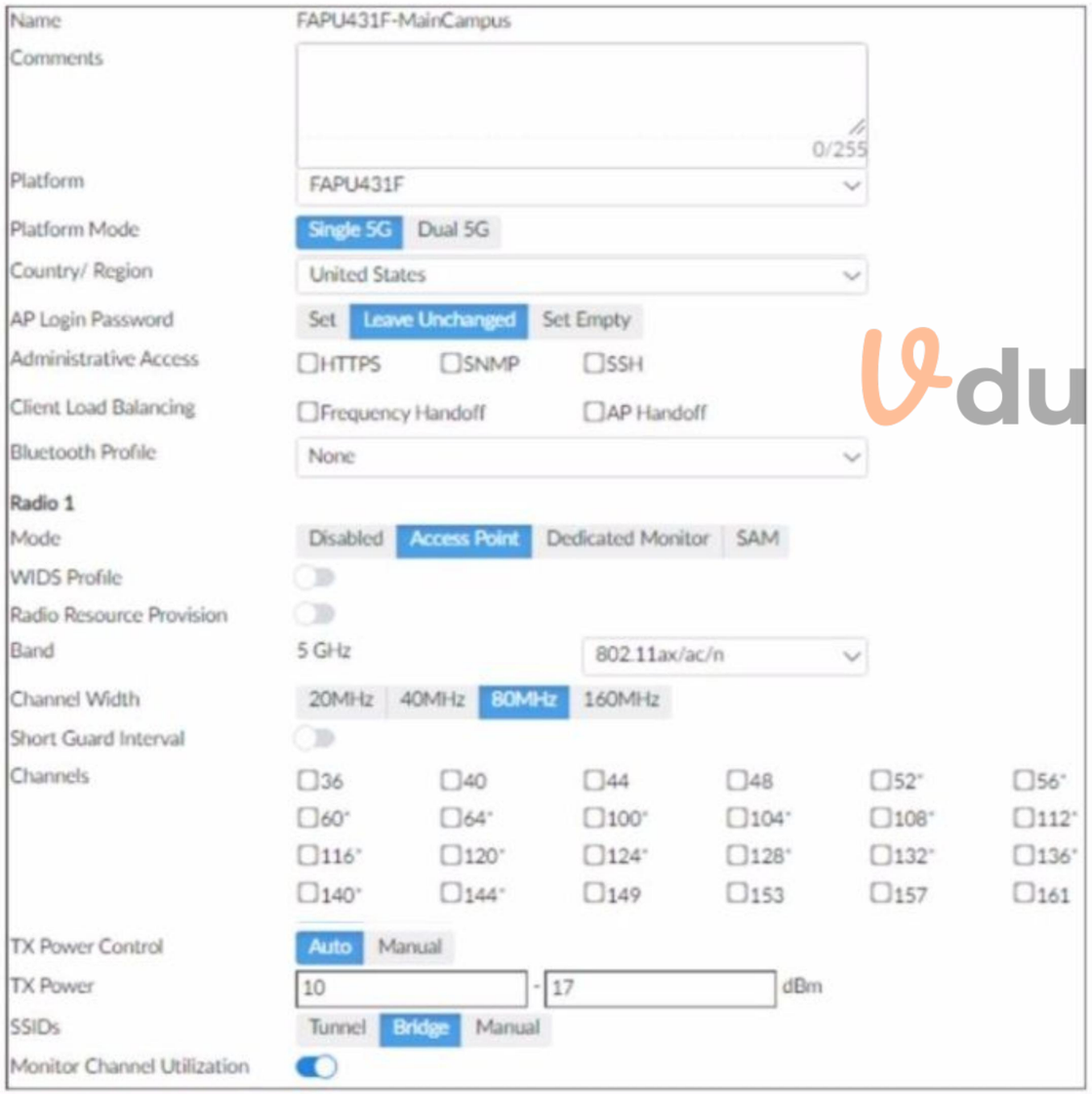
Correct Answer: A, B
Section:
Explanation:
According to the FortiGate Administration Guide, "To enable automated wireless client quarantine using IOC, you must configure the following settings: Configure your wireless network to be in tunnel mode. This allows FortiGate to inspect all wireless traffic 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.

QUESTION 9
Refer to the exhibits

SSID Profiles



AP Profile



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

Correct Answer: B
Section:
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.

QUESTION 10
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

Correct Answer: C, D
Section:
Explanation:
According to the FortiAuthenticator Administration Guide2, "The guest portal provides pre and post-log in services for users (such as password reset and token registration abilities), and rules and replacement messages can be configured." Therefore, option C is true. The same guide also states that "Administrators can use one or more incoming parameters to configure a mapping rule for the guest portal." Therefore, option D is true. Option A is false because remote users can sponsor any number of guest accounts, as long as they do not exceed the maximum number of guest accounts allowed by the license. Option B is false because administrators can choose to approve or reject guest accounts, or enable auto-approval.

QUESTION 11
Refer to the exhibit.

```
config wireless-controller wtp-profile
    edit "Main Networks - FAP-320C"
        set comment "Profile with standard networks"
        config platform
            set type 320C
        end
        set wan-port-mode wan-only
        set led-state enable
        set dtls-policy clear-text
        set max-clients 0
        set handoff-rssi 30
        set handoff-sta-thresh 30
        set handoff-roaming enable
        set ap-country GB
        set ip-fragment-preventing tcp-mss-adjust
        set tun-mtu-uplink 0
        set tun-mtu-downlink 0
        set split-tunneling-acl-path local
        set split-tunneling-acl-local-ap-subnet enable
        config split-tunneling-acl
            edit 1
                set dest-ip 192.168.5.0 255.255.255.0
            next
        end
        set allowaccess https ssh
        set login-passwd-change yes
        set lldp disable
```

Exhibit.

```
        config radio-1
            set mode ap
            set band 802.11n,g-only
            set protection-mode disable
            unset powersave-optimize
            set amsdu enable
            set coexistence enable
            set short-guard-interval disable
            set channel-bonding 20MHz
            set auto-power-level disable
            set power-level 100
            set dtim 1
            set beacon-interval 100
            set rts-threshold 2346
            set channel-utilization enable
            set spectrum-analysis disable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set max-clients 0
            set max-distance 0    next
config wireless-controller vap
    edit "Corporate"
        set ssid "Corporate"
        set passphrase ENC XXXX
        set schedule "always"
        set quarantine disable
    next
end
```

Refer to the exhibits
In the wireless configuration shown in the exhibits, an AP is deployed in a remote site and has a wireless network (VAP) called Corporate deployed to it

The network is a tunneled network however clients connecting to a wireless network require access to a local printer Clients are trying to print to a printer on the remote site but are unable to do so
Which configuration change is required to allow clients connected to the Corporate SSID to print locally?

A. Configure split-tunneling in the vap configuration
B. Configure split-tunneling in the wtp-profile configuration
C. Disable the Block Intra-SSID Traffic (intra-vap-privacy) setting on the SSID (VAP) profile
D. Configure the printer as a wireless client on the Corporate wireless network

Correct Answer: A
Section:
Explanation:
According to the Fortinet documentation1, "Split tunneling allows you to specify which traffic is tunneled to the FortiGate and which traffic is sent directly to the Internet. This can improve performance and reduce bandwidth usage." Therefore, by configuring split-tunneling in the vap configuration, you can allow the clients connected to the Corporate SSID to access both the corporate network and the local printer. Option B is incorrect because split-tunneling is configured at the vap level, not the wtp-profile level. Option C is incorrect because blocking intra-SSID traffic prevents wireless clients on the same SSID from communicating with each other, which is not related to accessing a local printer. Option D is unnecessary and impractical because the printer does not need to be a wireless client on the Corporate wireless network to be accessible by the clients.

QUESTION 12
Which two statements about FortiSwitch manager 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

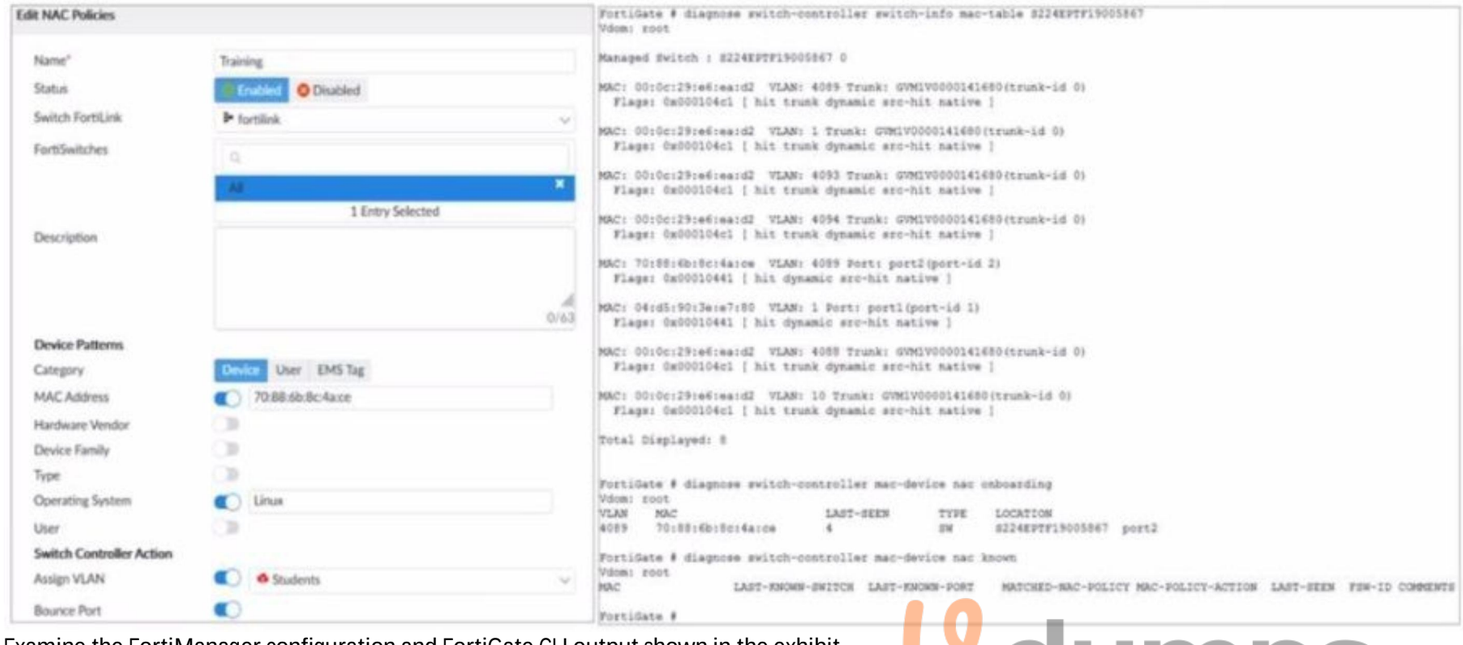
Correct Answer: B, C
Section:
Explanation:
According to the FortiManager Administration Guide1, "FortiManager obtains the FortiSwitch status information by querying the FortiGate REST API every three minutes." Therefore, option B is true because it describes how FortiManager gets the information about 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 any switch 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-manager2: https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/734537/fortiswitch-manager#fortiswitch-manager

QUESTION 13
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

Correct Answer: B, D
Section:
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.

QUESTION 14
Refer to the exhibit.

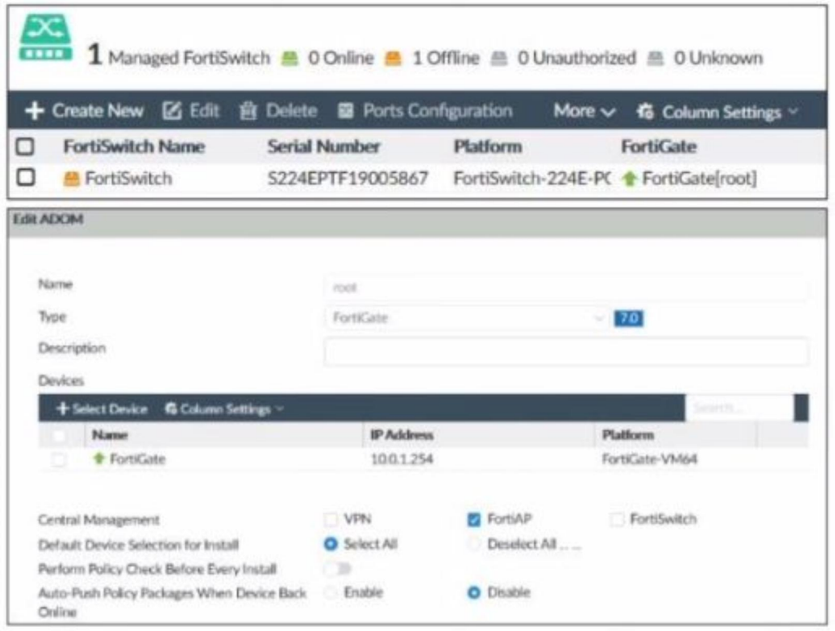


Examine the FortiManager configuration and FortiGate CLI output shown in the exhibit
An administrator is testing the NAC feature The test device is connected to a managed FortiSwitch device {S224EPTF19'537)onpOrt2
After applying the NAC policy on port2 and generating traffic on the test device the test 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

Correct Answer: A, B
Section:
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".

QUESTION 15
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

Correct Answer: C, D
Section:
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.

QUESTION 16
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

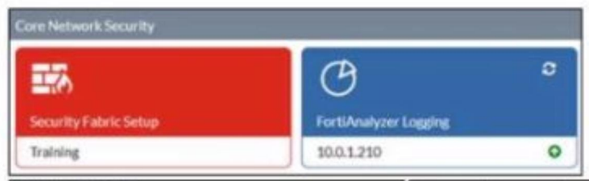
Correct Answer: A, C
Section:
Explanation:
According to the FortiAP Configuration Guide1, ''To enable the SSID, you must select at least one channel for the radio. If no channels are selected, the SSID will not be enabled. You must also enable Broadcast SSID.'' Therefore, option A is true because the 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

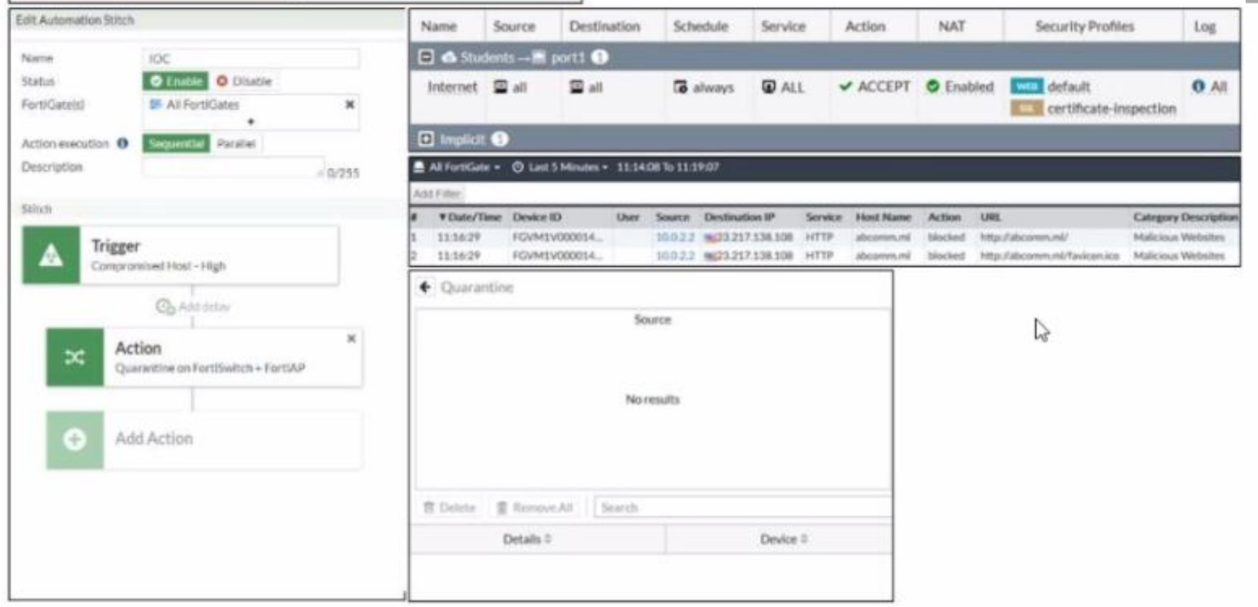
be broadcasting the SSID.According to the same guide1, "You can create AP groups and assign them to different locations or departments. You can then apply different settings, such as SSIDs, to each group." Option B is false because blocking intra-SSID traffic prevents wireless clients on the same SSID 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.

QUESTION 17
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

Correct Answer: D
Section:
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.

QUESTION 18
Refer to the exhibit.





Examine the FortiGate configuration FortiAnalyzer logs and FortiGate widget shown in the exhibit
An administrator is testing the Security Fabric quarantine automation The administrator added FortiAnalyzer to the Security Fabric and configured an automation stitch to automatically quarantine compromised devices The test device

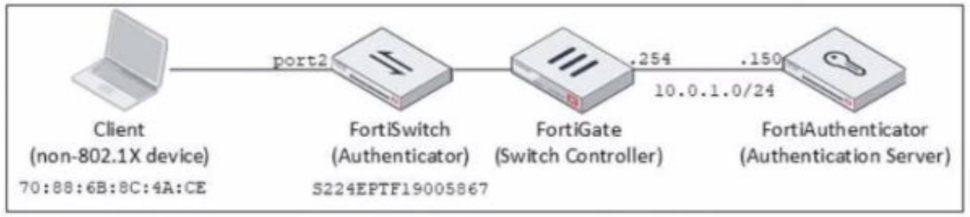
(::.:.:.!) s connected to a managed Fort Switch dev :e
After trying to access a malicious website from the test device, the administrator verifies that FortiAnalyzer has a log (or the test connection However the device is not getting quarantined by FortiGate as shown in the quarantine widget
Which two scenarios are likely to cause this issue? (Choose two)
A. The web filtering rating service is not working
B. FortiAnalyzer does not have a valid threat detection services license
C. The device does not have FortiClient installed
D. FortiAnalyzer does not consider the malicious website an indicator of compromise (IOC)

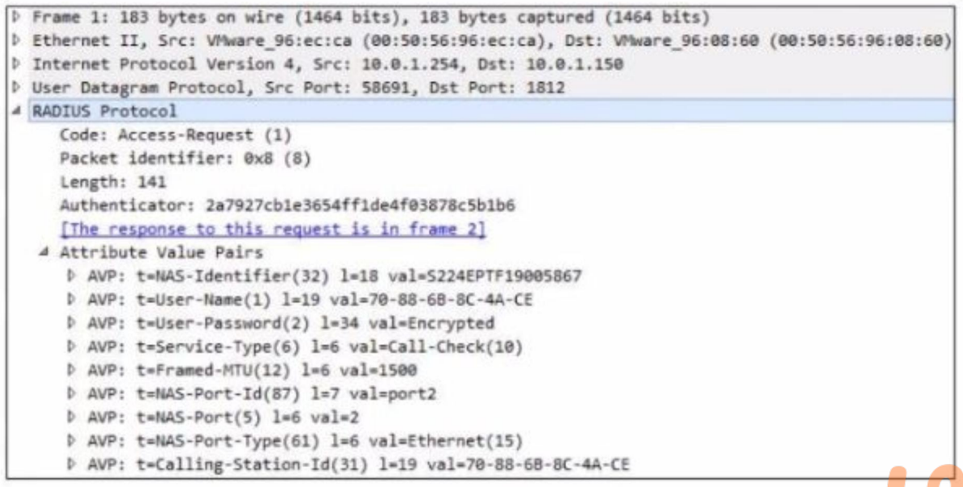
Correct Answer: B, D
Section:
Explanation:
According to the exhibits, the administrator has configured an automation stitch to automatically quarantine compromised devices based on FortiAnalyzer's threat detection services. However, according to the FortiAnalyzer logs, the test device is not detected as compromised by FortiAnalyzer, even though it tried to access a malicious website. Therefore, option B is true because FortiAnalyzer does not have a valid threat detection services license, which is required to enable the threat detection services feature. Option D is also true because FortiAnalyzer does not consider the malicious website an indicator of compromise (IOC), which is a criterion for identifying compromised devices. Option A is false because the web filtering rating service is working, as shown by the log entry that indicates that the test device accessed a URL with a category of ''Malicious Websites''. Option C is false because the device does not need to have FortiClient installed to be quarantined by FortiGate, as long as it is connected to a managed FortiSwitch device.

QUESTION 19
Which FortiSwitch VLANs are automatically created on FortGate when the first FortiSwitch device is discovered1?
A. default quarantine, rspan voice video onboarding and nac_segment
B. access, quarantine, rspan. voice, video, and onboarding
C. default quarantine rspan voice video and nac_segment
D. fortilink. quarantine erspan voice video and onboarding

Correct Answer: D
Section:
Explanation:
According to the FortiGate Administration Guide, ''When you add a FortiSwitch device to the Security Fabric, FortiGate automatically creates the following VLANs on the FortiSwitch device: fortilink, quarantine, erspan, voice, video, and onboarding.'' Therefore, option D is true because it lists the FortiSwitch VLANs that are automatically created on FortiGate when the first FortiSwitch device is discovered. Option A is false because default and nac_segment are not among the automatically created VLANs. Option B is false because access and rspan are not among the automatically created VLANs. Option C is false because default and nac_segment are not among the automatically created VLANs.

QUESTION 20
Refer to the exhibit.



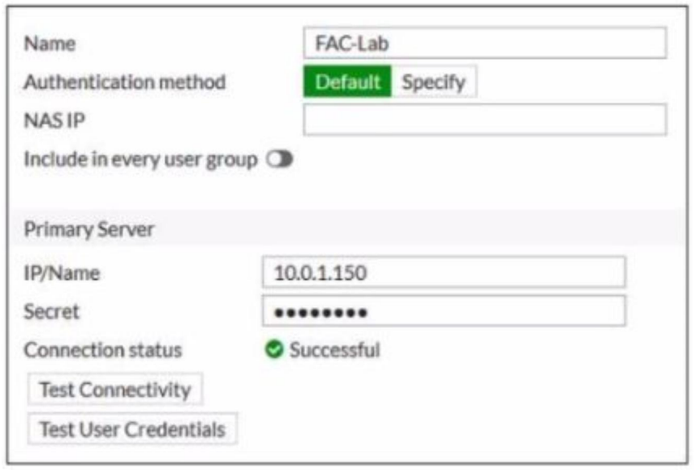


Examine the network diagram and packet capture shown in the exhibit
The packet capture was taken between FortiGate and FortiAuthenticator and shows a RADIUS Access-Request packet sent by FortiSwitch to FortiAuthenticator through FortiGate
Why does the User-Name attribute in the RADIUS Access-Request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

Correct Answer: B
Section:
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.

QUESTION 21
Refer to the exhibit.



Examine the RADIUS server configuration shown in the exhibit
An administrator has configured a RADIUS server on FortiGate that points to FortiAuthenticator FortiAuthenticator is acting as an authentication proxy and is configured to relay all authentication requests to a remote Windows AD server using LDAP
While testing the configuration the administrator noticed that the 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

Correct Answer: A, C
Section:
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.