Exam Questions NSE7_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0

https://www.2passeasy.com/dumps/NSE7_LED-7.0/

NEW QUESTION 1
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, rspa
C. voice, video, and onboarding
D. default quarantine rspan voice video and nac_segment
E. fortilin
F. quarantine erspan voice video and onboarding

Answer: D

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

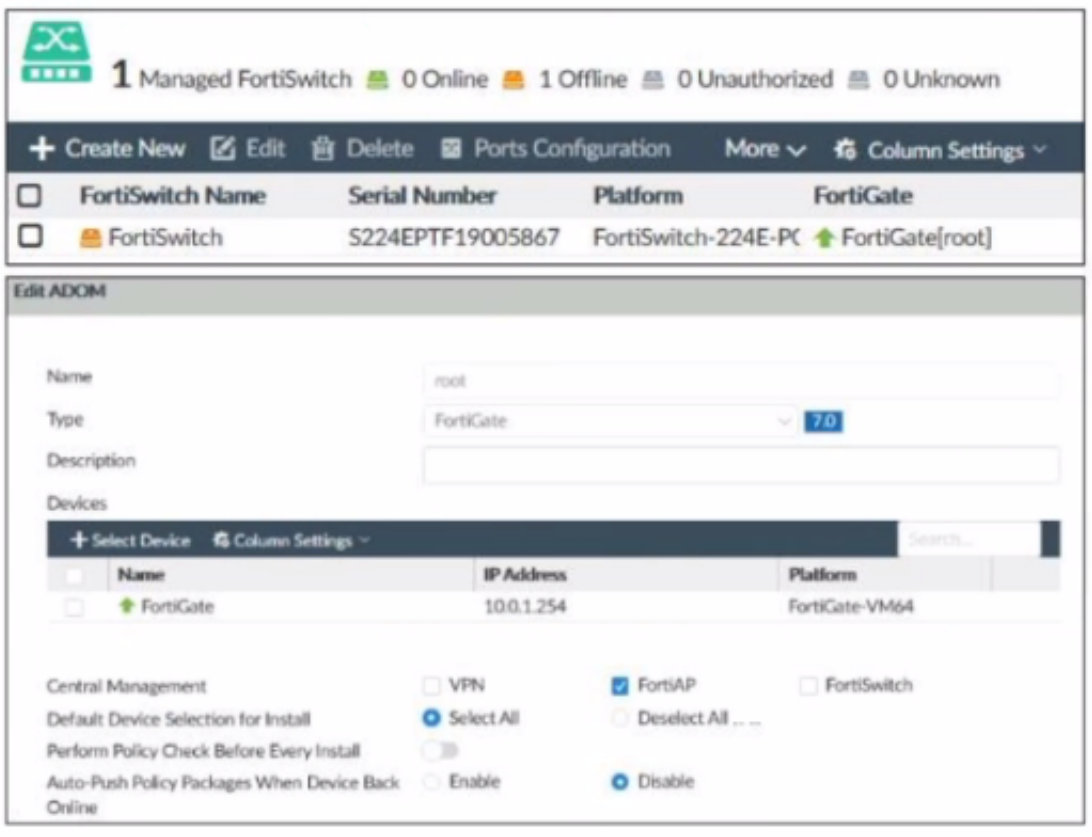
NEW QUESTION 2
Where can FortiGate learn the FortiManager IP address or FQDN for zero-touch provisioning'?

A. From an LDAP server using a simple bind operation
B. From a TFTP server
C. From a DHCP server using options 240 and 241
D. From a DNS server using A or AAAA records

Answer: D

Explanation:
According to the FortiGate Administration Guide, “FortiGate can learn the FortiManager IP address or FQDN for zero-touch provisioning from a DNS server using A or AAAA records. The DNS server must be configured to resolve the hostname fortimanager.fortinet.com to the IP address or FQDN of the FortiManager device.” Therefore, option D is true because it describes the method for FortiGate to learn the FortiManager IP address or FQDN for zero-touch provisioning. Option A is false because LDAP is not used for zero-touch provisioning. Option B is false because TFTP is not used for zero-touch provisioning. Option C is false because DHCP options 240 and 241 are not used for zero-touch provisioning.

NEW QUESTION 3
Refer to the exhibit.



Examine the FortiManager information shown in the exhibit
Which two statements about the FortiManager status are true" (Choose two)

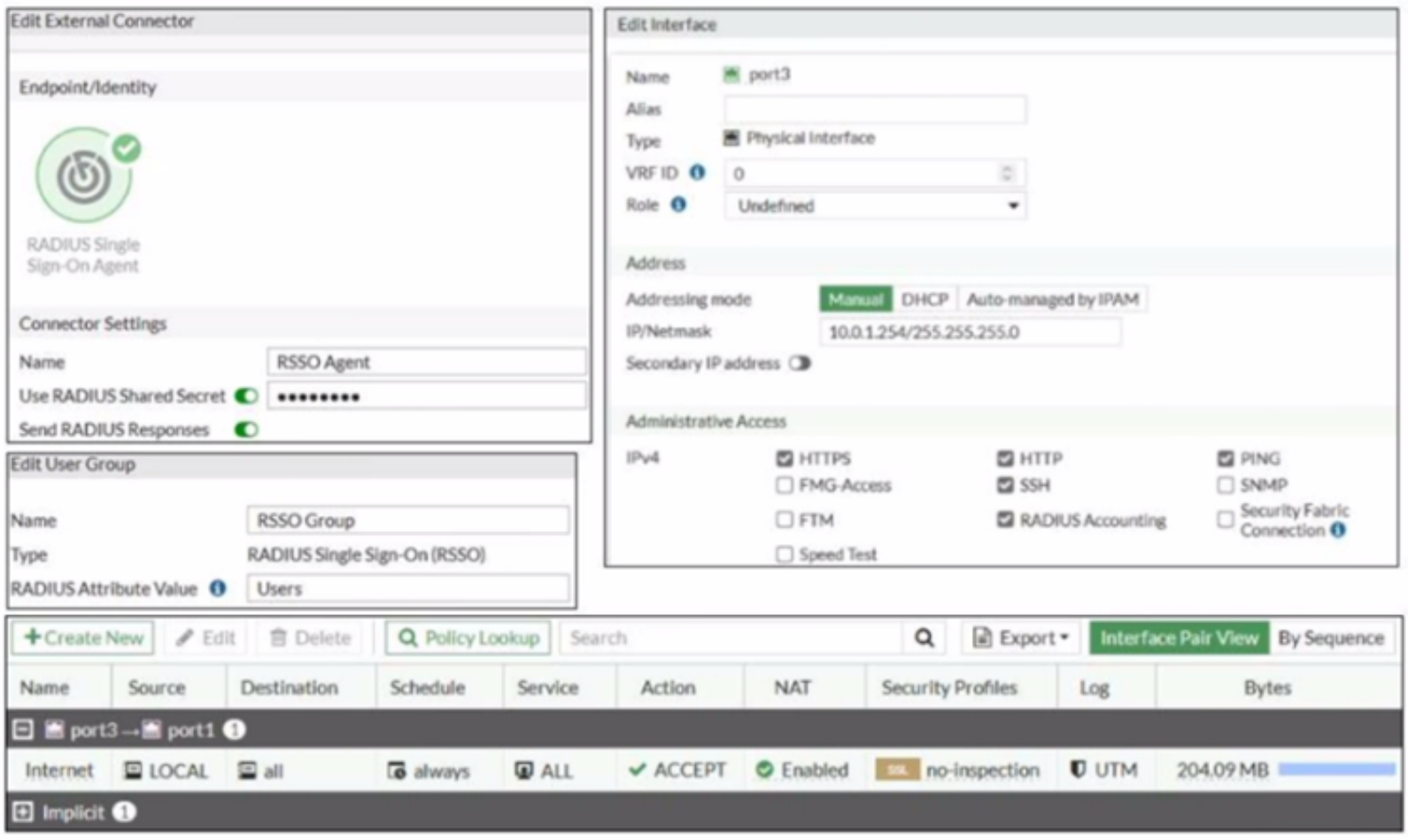
A. FortiSwitch manager is working in per-device management mode
B. FortiSwitch is not authorized
C. FortiSwitch manager is working in central management mode
D. FortiSwitch is authorized and offline

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 4
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 5
What is the purpose of enabling Windows Active Directory Domain Authentication on FortiAuthenticator?

A. It enables FortiAuthenticator to use Windows administrator credentials to perform an LDAP lookup for a user search
B. It enables FortiAuthenticator to use a Windows CA certificate when authenticating RADIUS users
C. It enables FortiAuthenticator to import users from Windows AD
D. It enables FortiAuthenticator to register itself as a Windows trusted device to proxy authentication using Kerberos

Answer: D

Explanation:
According to the FortiAuthenticator Administration 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 6
Which two statements about FortiSwitchmanager are true1? (Choose two)

A. Per-device management is the default management mode on FortiManager
B. FortiManager obtains the FortiSwitch status information by querying the FortiGate REST API every three minutes
C. If the administrator makes any changes on FortiSwitch manager they must also install those changes on FortiGate so that those changes are applied on the managed switches
D. Any switch discovered or authorized on FortiGate must be added manually on FortiSwitch manager

Answer: BC

Explanation:
According to the FortiManager Administration Guide1, “FortiManager obtains the FortiSwitch status information by querying the FortiGate REST API every three minutes.” Therefore, option B is true because it describes how FortiManager gets the information about the managed switches. According to the same guide2, “If you make any changes in this module, you must install them on your managed device so that they are applied on your managed switches.” Therefore, option C is true because it describes what the administrator must do after making any changes on FortiSwitch manager. Option A is false because central management is the default management mode on FortiManager, not per-device management. Option D is false because anyswitch discovered or authorized on FortiGate will be automatically added on FortiSwitch manager, not manually.
1: https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/734537/fortiswitch-manager 2: https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/734537/fortiswitch-manager#fortisw

NEW QUESTION 7
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 8
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 IX 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

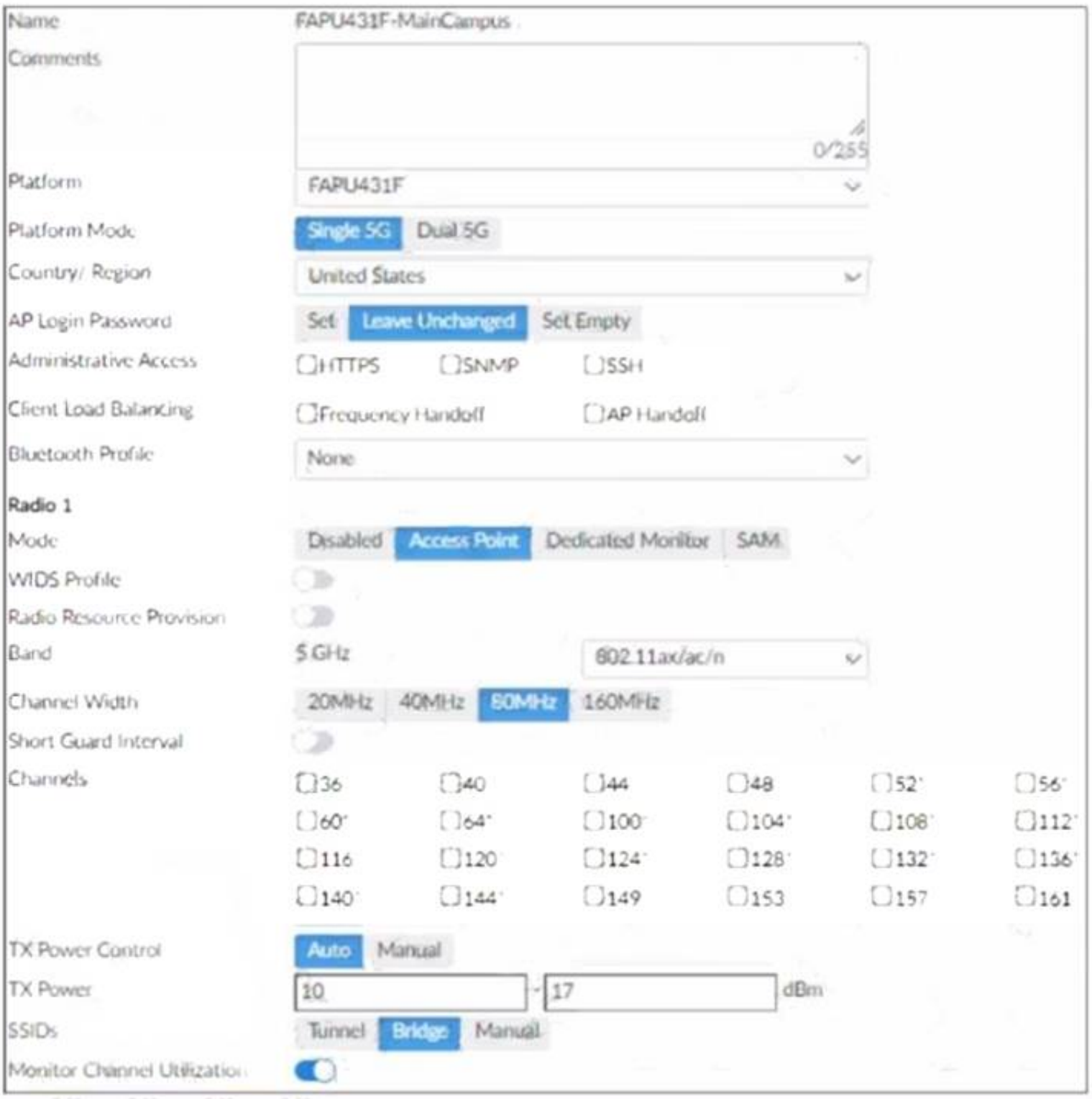
Answer: AD

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 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

Answer: B

Explanation:
According to the FortiManager Administration Guide1, “To enable the SSID, you must select at least one channel for the radio. If no channels are selected, the SSID will not be enabled.” Therefore, enabling one channel in the Channels section will allow the SSIDs to broadcast.

NEW QUESTION 10
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

Answer: C

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

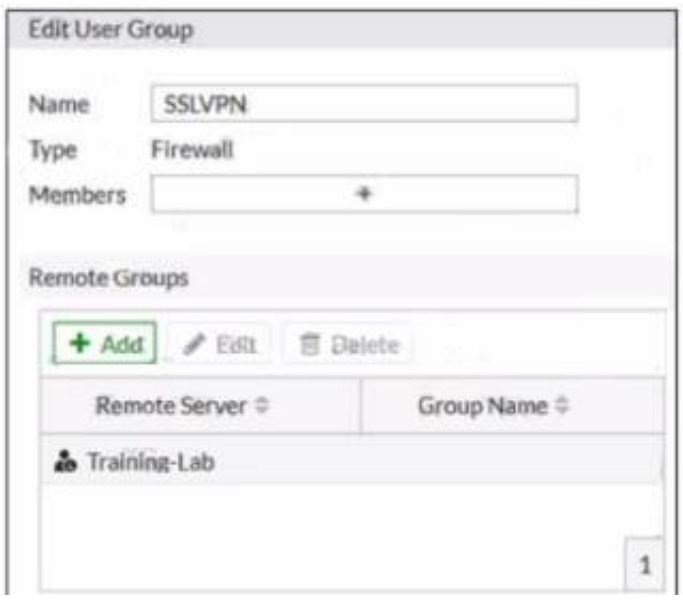
NEW QUESTION 10
Which EAP method requires the use of a digital certificate on both the server end and the client end?

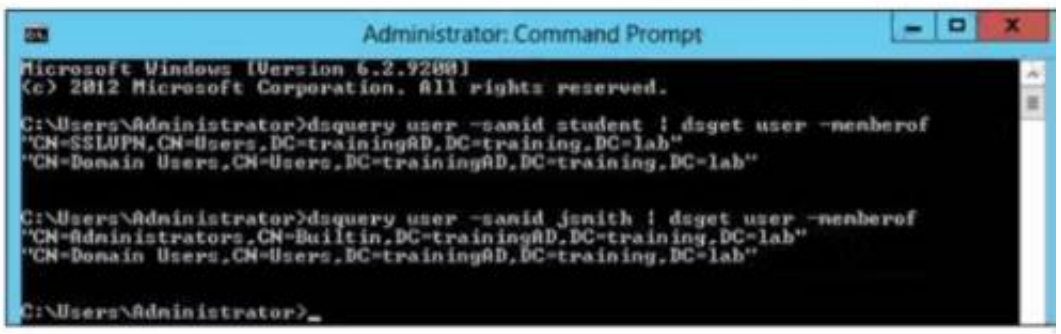
A. EAP-TTLS
B. PEAP
C. EAP-GTC
D. EAP-TLS

Answer: D

Explanation:
According to the FortiGate Administration Guide, “EAP-TLS is the most secure EAP method. It requires a digital certificate on both the server end and the client end. The server and client authenticate each other using
their certificates.” Therefore, option D is true because it describes the EAP method that requires the use of a digital certificate on both the server end and the client end. Option A is false because EAP-TTLS only requires a digital certificate on the server end, not the client end. Option B is false because PEAP also only requires a digital certificate on the server end, not the client end. Option C is false because EAP-GTC does not require a digital certificate on either the server end or the client end.

NEW QUESTION 13
Refer to the exhibit.





Examine the FortiGate user group configuration and the Windows AD LDAP group membership information shown in the exhibit
FortiGate is configured to authenticate SSL VPN users against Windows AD using LDAP The administrator configured the SSL VPN user group for SSL VPN users However the administrator noticed that both the student and j smith users can connect to SSL VPN

Which change can the administrator make on FortiGate to restrict the SSL VPN service to the student user only?

A. In the SSL VPN user group configuration set Group Nam© to CN-SSLVPN, CN="users, DC-trainingAD, DC-training, DC-lab
B. In the SSL VPN user group configuration, change Name to cn=sslvpn, CN=users, DC=trainingAD, Detraining, DC-lab.
C. In the SSL VPN user group configuration set Group Name to :::=Domain users.CN-Users/DC=trainingAD, DC-training, DC=lab.
D. In the SSL VPN user group configuration change Type to Fortinet Single Sign-On (FSSO)

Answer: A

Explanation:
According to the FortiGate Administration Guide, “The Group Name is the name of the LDAP group that you want to use for authentication. The name must match exactly the name of the LDAP group on the LDAP server.” Therefore, option A is true because it will set the Group Name to match the LDAP group that contains only the student user. Option B is false because changing the Name will not affect the authentication process, as it is only a local identifier for the user group on FortiGate. Option C is false because setting the Group Name to Domain Users will include all users in the domain, not just the student user. Option D is false because changing the Type to FSSO will require a different configuration method and will not solve the problem.

NEW QUESTION 17
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_LED-7.0 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_LED-7.0 Product From:

https://www.2passeasy.com/dumps/NSE7_LED-7.0/

Money Back Guarantee

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