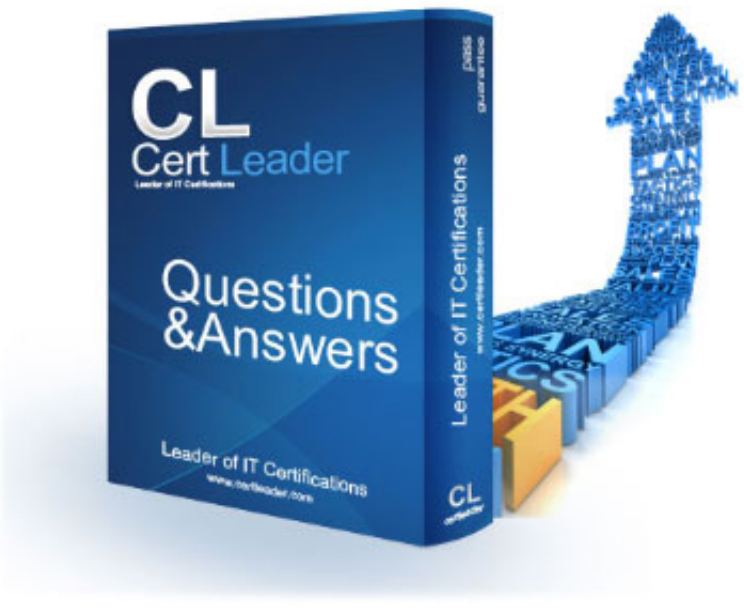
NSE7_LED-7.0 Dumps

Fortinet NSE 7 - LAN Edge 7.0

https://www.certleader.com/NSE7_LED-7.0-dumps.html



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.

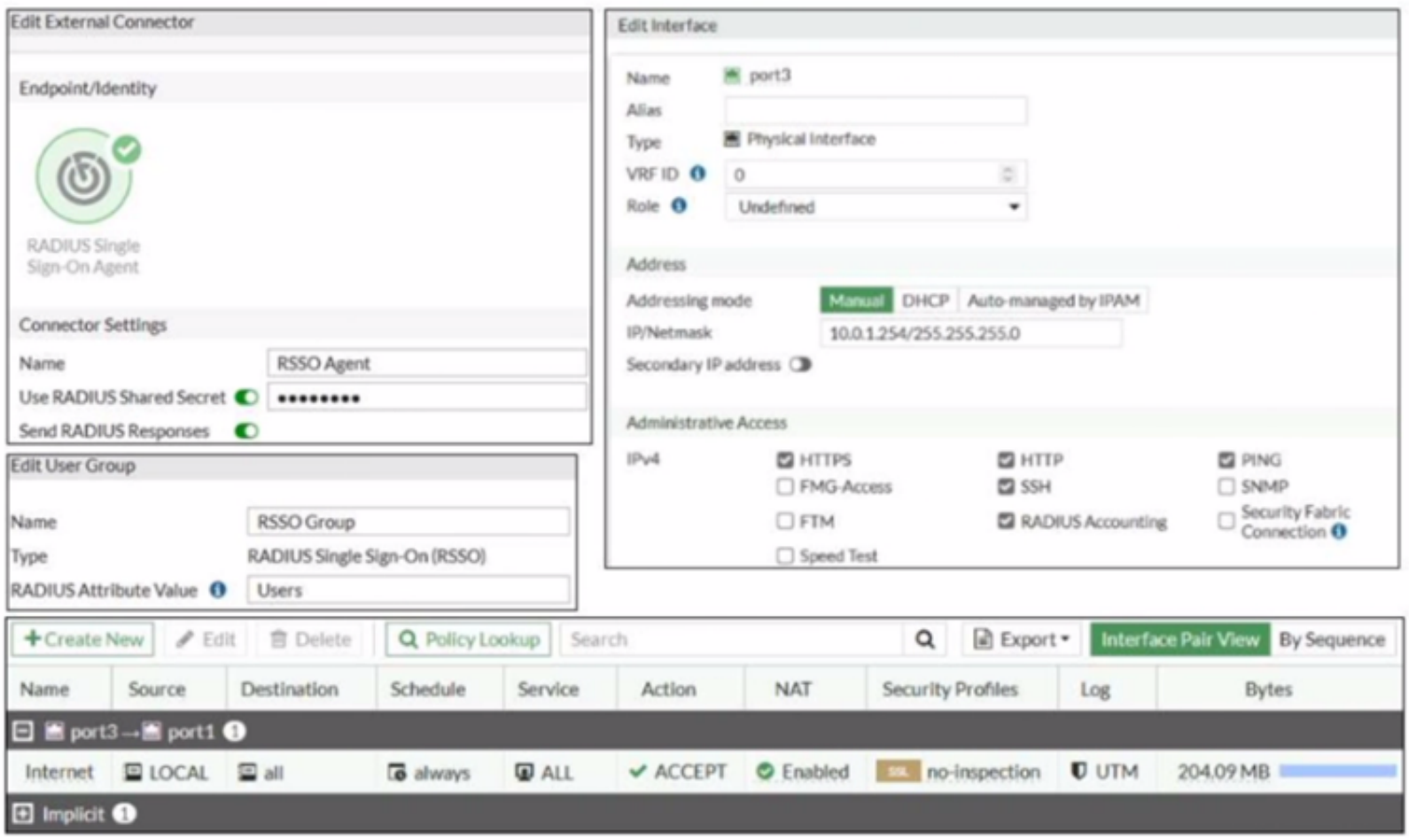
NEW QUESTION 2
Where can FortiGate learn the FortiManager IP address or FQDN for zero-touch provisioning'?

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 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 4
Which two statements about MAC address quarantine by redirect mode are true? (Choose two)

A. The quarantined device is moved to the quarantine VLAN
B. The device MACaddress is added to the Quarantined Devices firewall address group
C. It is the default mode for MAC address quarantine
D. The quarantined device is kept in the current VLAN

Answer: BD

Explanation:
According to the FortiGate Administration Guide, “MAC address quarantine by redirect mode allows you to quarantine devices by adding their MAC addresses to a firewall address group called Quarantined Devices. The quarantined devices are kept in their current VLANs, but their traffic is redirected to a quarantine portal.” Therefore, options B and D are true because they describe the statements about MAC address quarantine by redirect mode. Option A is false because the quarantined device is not moved to the quarantine VLAN, but rather kept in the current VLAN. Option C is false because redirect mode is not the default mode for MAC address quarantine, but rather an alternative mode that can be enabled by setting mac-quarantine-mode to redirect.
https://docs.fortinet.com/document/fortiap/7.0.0/configuration-guide/734537/radius-authenticated-dynamic-vlan
: https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/734537/mac-address-quarantine

NEW QUESTION 5
Refer to the exhibits.

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

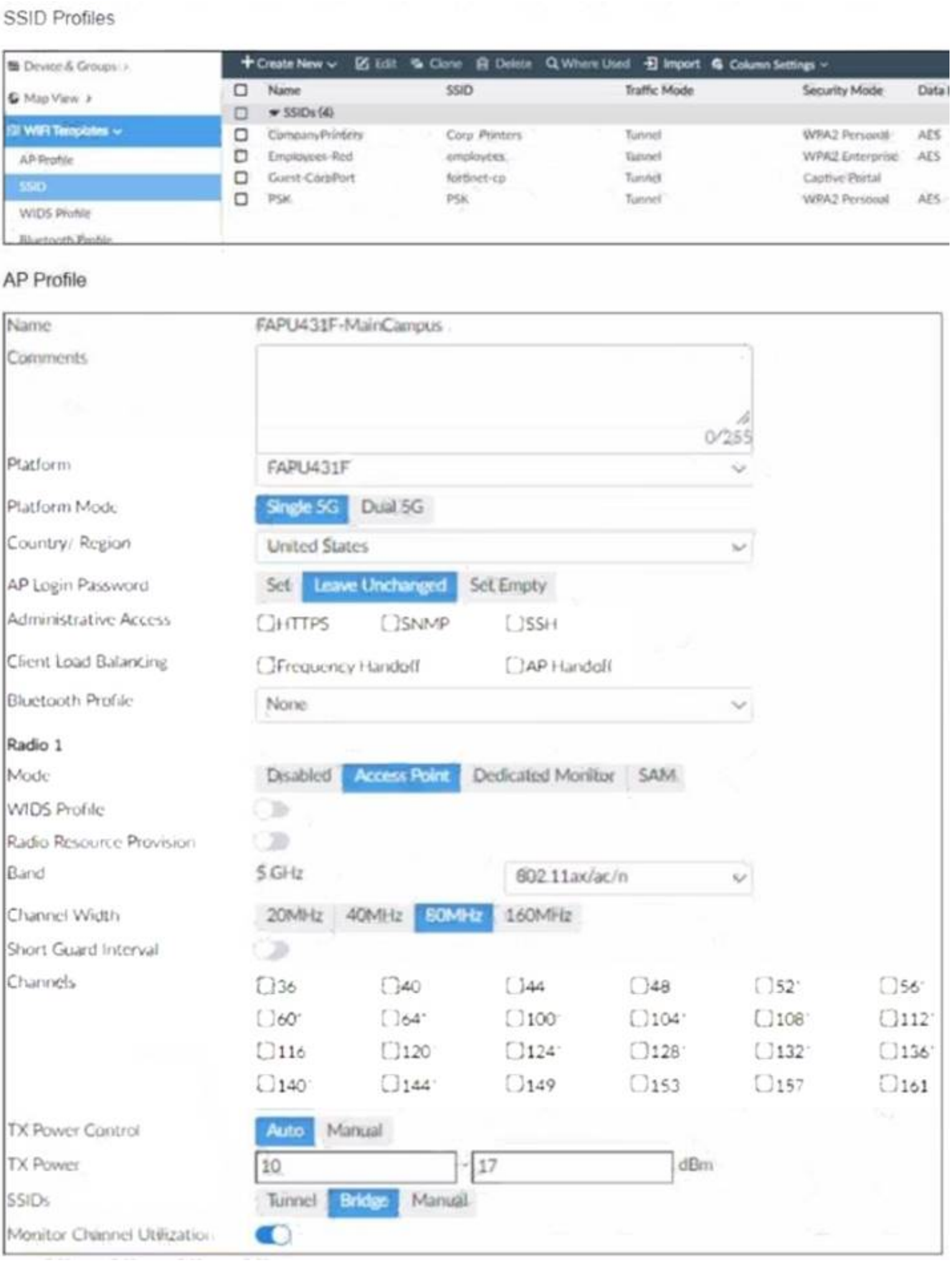
A. Change the AP 2 4 GHz channel to 11
B. Change the AP 2 4 GHz channel to 1.
C. Change the AP 2 4 GHz channel to 9.
D. Change the AP 2 4 GHz channel to 13.

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 6
Refer to the exhibits



The exhibits show the wireless network (VAP) SSID profiles defined on FortiManager and an AP profile assigned to a group of APs that are supported by FortiGate None of the APs are broadcasting the SSIDs defined by the AP profile
Which changes do you need to make to enable the SSIDs to broadcast?

A. In the SSIDs section enable Tunnel
B. Enable one channel in the Channels section
C. Enable multiple channels in the Channels section and enable Radio Resource Provision
D. In the SSIDs section enable Manual and assign the networks manually

Answer: B

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

NEW QUESTION 7
You are setting up an SSID (VAP) to perform RADIUS-authenticated dynamic VLAN allocation Which three RADIUS attributes must be supplied by the RADIUS server to enable successful VLAN

allocation" (Choose three.)

A. Tunnel-Private-Group-ID
B. Tunnel-Pvt-Group-ID
C. Tunnel-Preference
D. Tunnel-Type
E. Tunnel-Medium-Type

Answer: ADE

Explanation:
According to the FortiAP Configuration Guide, "To perform RADIUS-authenticated dynamic VLAN allocation, the RADIUS server must supply the following RADIUS attributes: Tunnel-Private-Group-ID, which specifies the VLAN ID to assign to the user. Tunnel-Type, which specifies the tunneling protocol used for the VLAN. The value must be 13 (VLAN). Tunnel-Medium-Type, which specifies the transport medium used for the VLAN. The value must be 6 (802). Therefore, options A, D, and E are true because they describe the RADIUS attributes that must be supplied by the RADIUS server to enable successful VLAN allocation. Option B is false because Tunnel-Pvt-Group-ID is not a valid RADIUS attribute name, but rather a typo for Tunnel-Private-Group-ID. Option C is false because Tunnel-Preference is not a required RADIUS attribute for dynamic VLAN allocation, but rather an optional attribute that specifies the priority of the VLAN.

NEW QUESTION 8
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
```

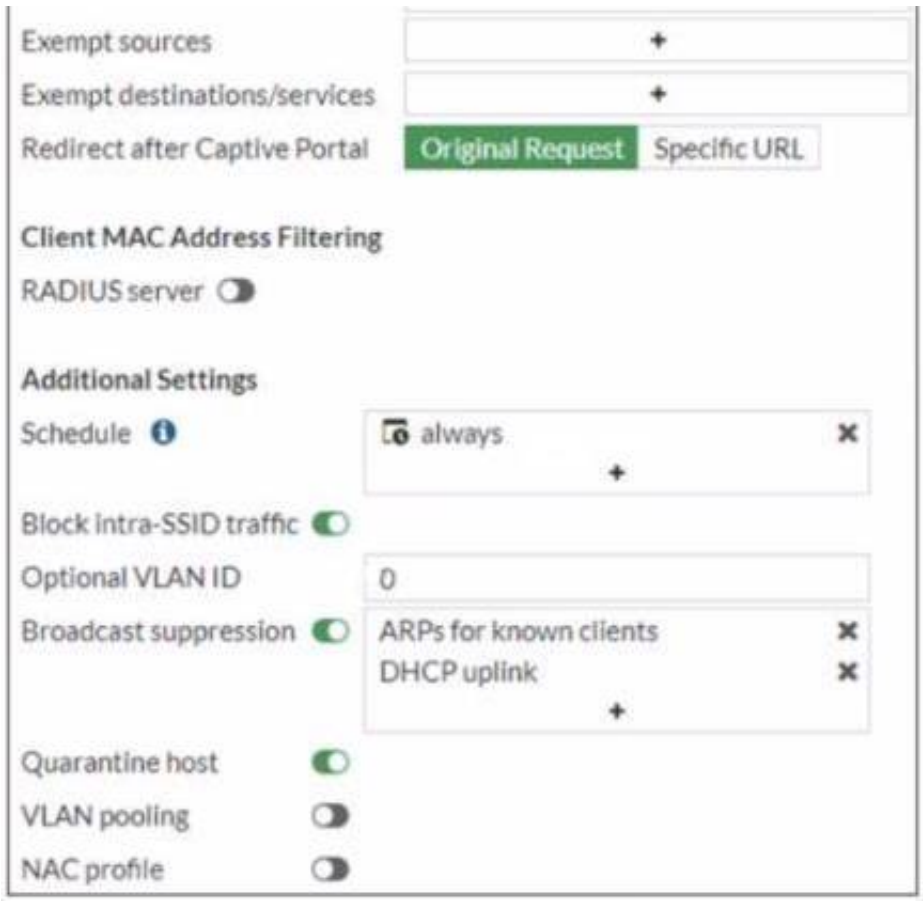
By default FortiOS creates the following DHCP server scope for the FortiLink interface as shown in the exhibit
What is the objective of the vci-string setting?

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

Answer: C

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.

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 captivs-portal-exempt option in the firewall policy with the ID 11.
C. Apply a guest.portal user group in the firewall policy with the ID 11.
D. Include the wireless client subnet range in the Exempt Source section

Answer: C

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

NEW QUESTION 10
When you configure a FortiAP wireless interface for auto TX power control which statement describes how it configures its transmission power"?

A. Every 30 seconds the AP will measure the signal strength of the AP using the client The AP will adjust its signal strength up or down until the AP signal is detected at -70 dBm
B. Every 30 seconds FortiGate measures the signal strength of adjacent AP interfaces It will adjust its own AP power to match the adjacent AP signal strength
C. Every 30 seconds FortiGate measures the signal strength of adjacent FortiAP interfaces It will adjust the adjacent AP power to be detectable at -70 dBm
D. Every 30 seconds FortiGate measures the signal strength of the weakest associated client The AP will then configure its radio power to match the detected signal strength of the client

Answer: A

Explanation:
According to the FortiAP Configuration Guide1, “Auto TX power control allows the AP to adjust its transmit power based on the signal strength of the client. The AP will measure the signal strength of the client every 30 seconds and adjust its transmit power up or down until the client signal is detected at -70 dBm.” Therefore, option A is true because it describes how the FortiAP wireless interface configures its transmission power when auto TX power control is enabled. Option B is false because FortiGate does not measure the signal strength of adjacent AP interfaces, but rather the FortiAP does. Option C is false because FortiGate does not
adjust the adjacent AP power, but rather the FortiAP adjusts its own power. Option D is false becauseFortiGate does not measure the signal strength of the weakest associated client, but rather the FortiAP does.

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.

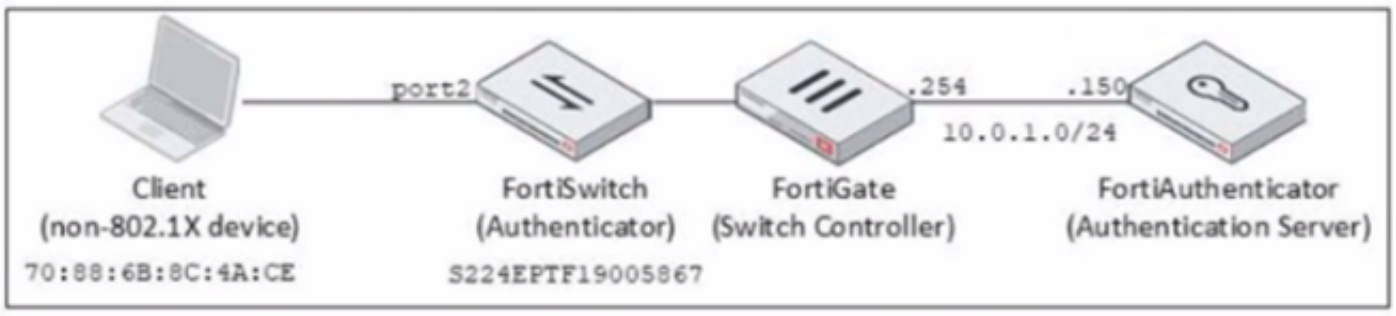
NEW QUESTION 14
Which CLI command should an administrator use to view the certificate verification process in real time?

A. diagnose debug application foauthd -1
B. diagnose debug application radiusd -1
C. diagnose debug application authd -1
D. diagnose debug application fnbamd -1

Answer: A

Explanation:
According to the FortiOS CLI Reference Guide, “The diagnose debug application foauthd command enables debugging of certificate verification process in real time.” Therefore, option A is true because it describes the CLI command that an administrator should use to view the certificate verification process in real time. Option B is false because diagnose debug application radiusd -1 enables debugging of RADIUS authentication process, not certificate verification process. Option C is false because diagnose debug application authd -1 enables debugging of authentication daemon process, not certificate verification process. Option D is false because diagnose debug application fnbamd -1 enables debugging of FSSO daemon process, not certificate verification process.

NEW QUESTION 18
Refer to the exhibit.




```
Frame 1: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Ethernet II, Src: VMware_96:ec:ca (00:50:56:96:ec:ca), Dst: VMware_96:08:60 (00:50:56:96:08:60)
Internet Protocol Version 4, Src: 10.0.1.254, Dst: 10.0.1.150
User Datagram Protocol, Src Port: 58691, Dst Port: 1812
RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x8 (8)
    Length: 141
    Authenticator: 2a7927cb1e3654ff1de4f03878c5b1b6
    [The response to this request is in frame 2]
  Attribute Value Pairs
    AVP: t=NAS-Identifier(32) l=18 val=S224EPTF19005867
    AVP: t=User-Name(1) l=19 val=70-88-6B-8C-4A-CE
    AVP: t=User-Password(2) l=34 val=Encrypted
    AVP: t=Service-Type(6) l=6 val=Call-Check(10)
    AVP: t=Framed-MTU(12) l=6 val=1500
    AVP: t=NAS-Port-Id(87) l=7 val=port2
    AVP: t=NAS-Port(5) l=6 val=2
    AVP: t=NAS-Port-Type(61) l=6 val=Ethernet(15)
    AVP: t=Calling-Station-Id(31) l=19 val=70-88-6B-8C-4A-CE
```

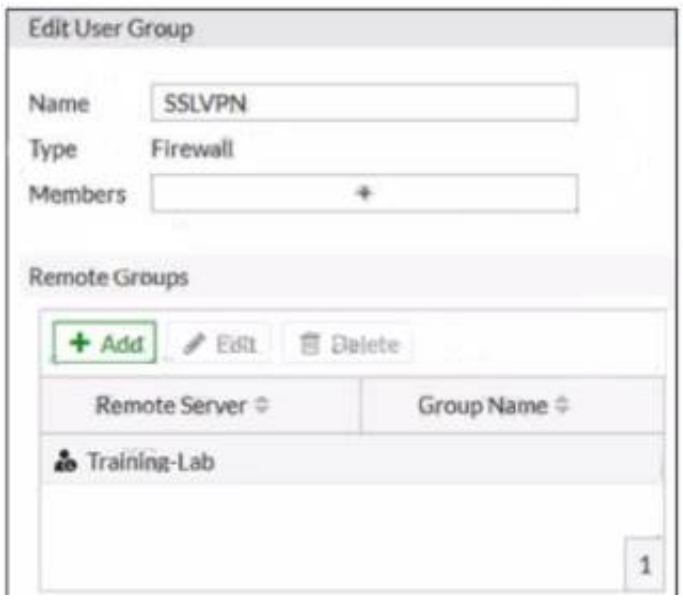
Examine the network diagram and packet capture shown in the exhibit
The packet capture was taken between FortiGate and FortiAuthenticator and shows a RADIUS Access-Request packet sent by FortiSwitch to FortiAuthenticator through FortiGate
Why does the User-Name attribute in the RADIUS Access-Request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

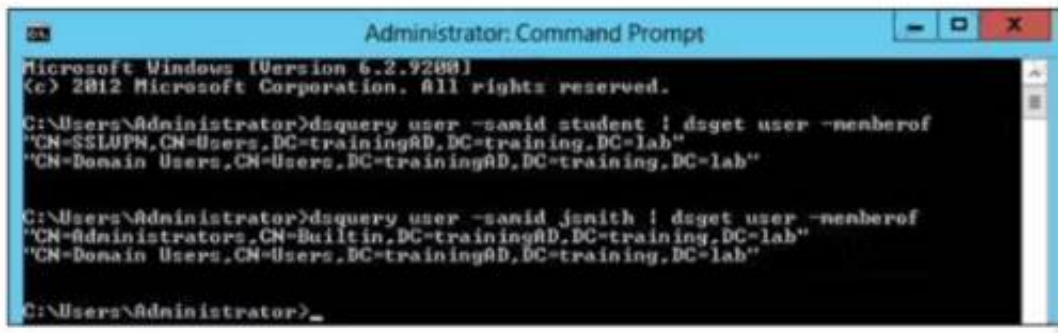
A. The client is performing AD machine authentication
B. FortiSwitch is authenticating the client using MAC authentication bypass
C. The client is performing user authentication
D. FortiSwitch is sending a RADIUS accounting message to FortiAuthenticator

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 20
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 22
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE7_LED-7.0 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE7_LED-7.0-dumps.html