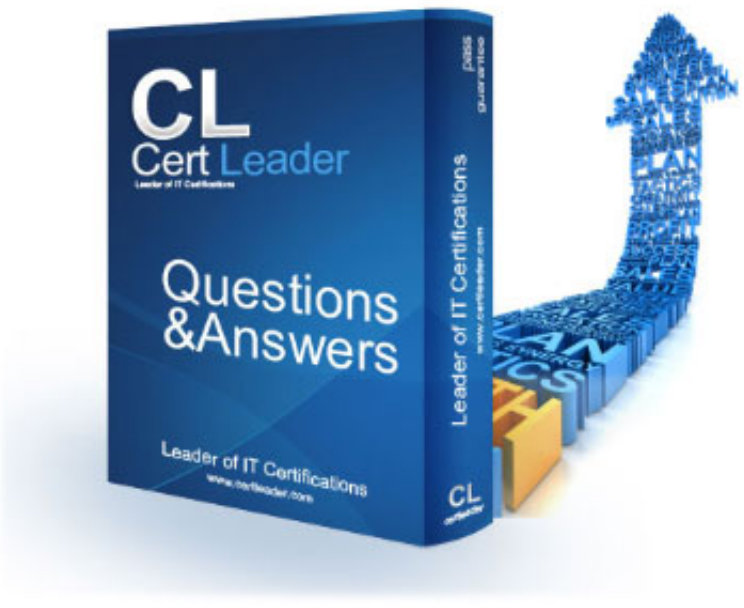
NSE7_LED-7.0 Dumps

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.

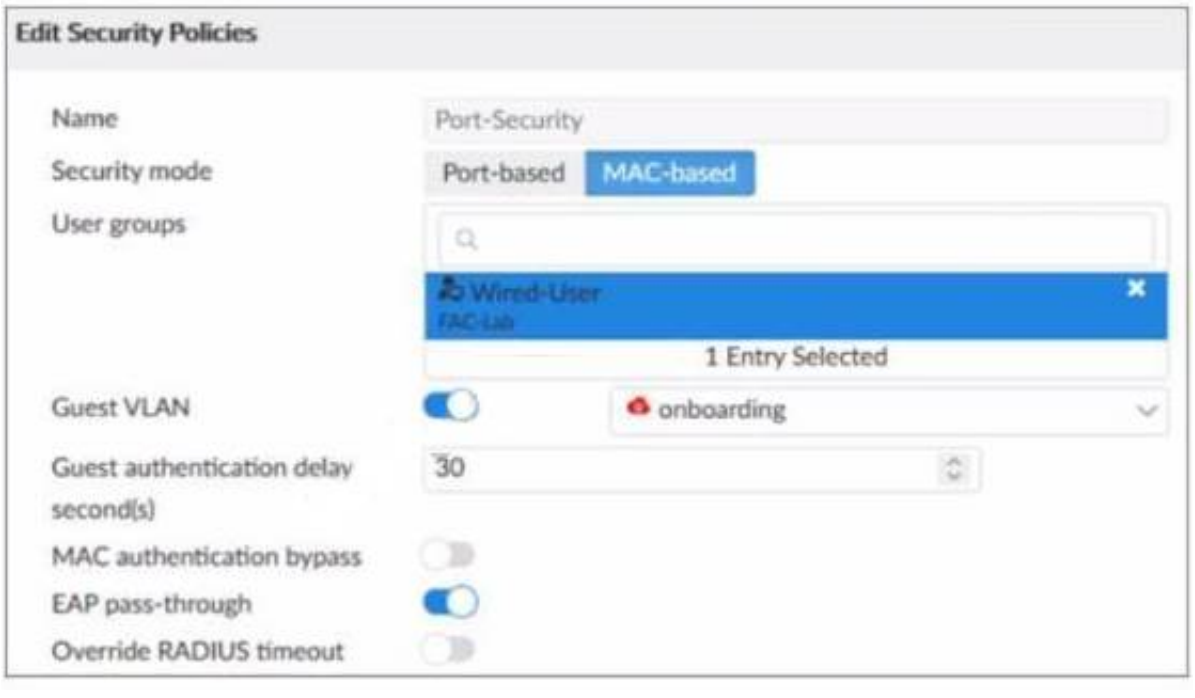
NEW QUESTION 3
Which two statements about MAC address quarantine by redirect mode are true? (Choose two)

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 4
Refer to the exhibit.



Examine the FortiSwitch security policy shown in the exhibit

If the security profile shown in the exhibit is assigned to all ports on a FortiSwitch device for 802 1X authentication which statement about the switch is correct?

A. FortiSwitch cannot authenticate multiple devices connected to the same port
B. FortiSwitch will try to authenticate non-802 1X devices using the device MAC address as the username and password
C. FortiSwitch will assign non-802 1X devices to the onboarding VLAN
D. All EAP messages will be terminated on FortiSwitch

Answer: C

Explanation:
According to the FortiSwitch Administration Guide, “If a device does not support 802.1X authentication, you can configure the switch to assign the device to an onboarding VLAN. The onboarding VLAN is a separate VLAN that you can use to provide limited network access to non-802.1X devices.” Therefore, option C is true because it describes the behavior of FortiSwitch when the security profile shown in the exhibit is assigned to all ports. Option A is false because FortiSwitch can authenticate multiple devices connected to the same port using MAC-based or MAB-EAP modes. Option B is false because FortiSwitch will not try to authenticate non-802.1X devices using the device MAC address as the username and password, but rather use MAC authentication bypass (MAB) or EAP pass-through modes. Option D is false because all EAP messages will be terminated on FortiGate, not FortiSwitch, when using 802.1X authentication.

NEW QUESTION 5
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 6
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
```

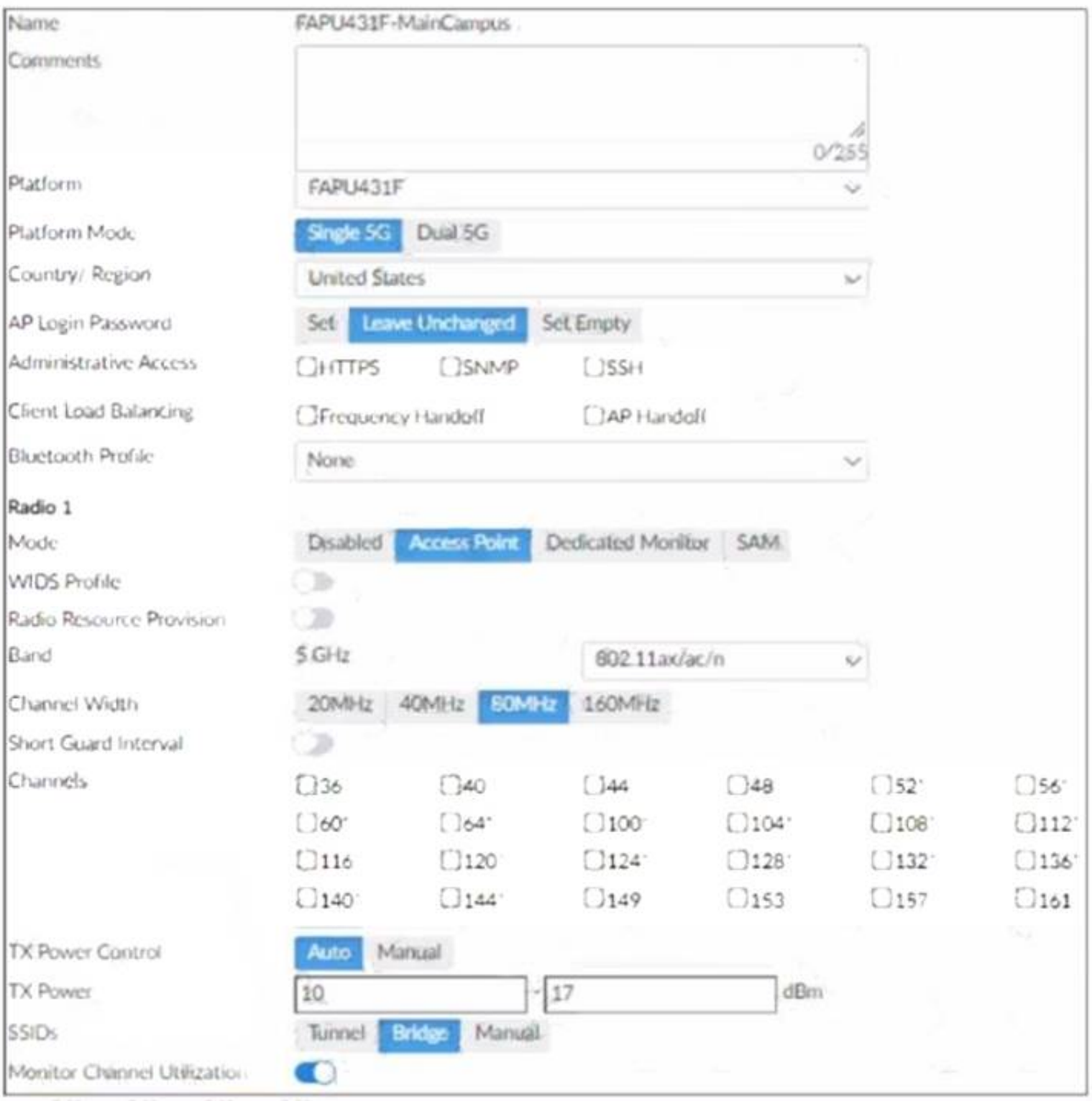
Refer to the exhibits
In the wireless configuration shown in the exhibits, an AP is deployed in a remote site and has a wireless network (VAP) called Corporate deployed to it
The network is a tunneled network however clients connecting to a wireless network require access to a local printer Clients are 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

Answer: A

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.

NEW QUESTION 7
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 8
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

Answer: AC

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.

NEW QUESTION 9
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.

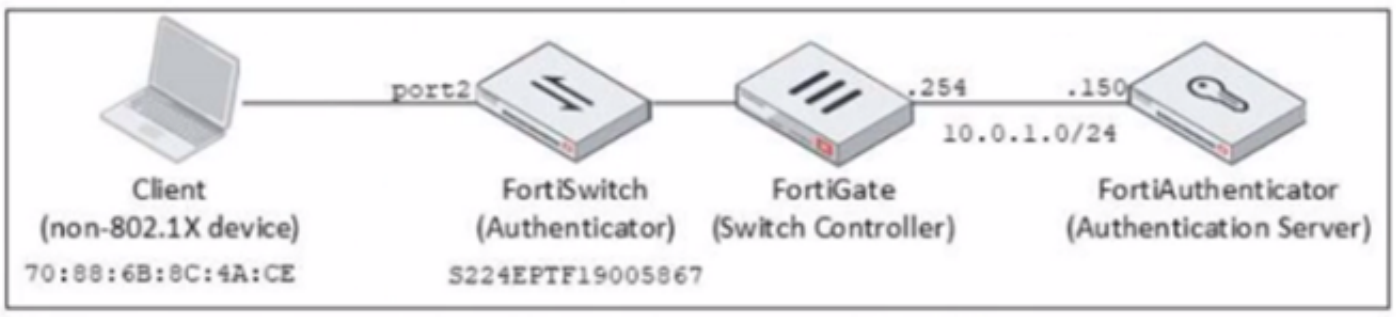
NEW QUESTION 10
A wireless network in a school provides guest access using a captive portal to allow unregistered users to self-register and access the network The administrator is requested to update the existing configuration to provide captive portal authentication through a secure connection (HTTPS)
Which two changes must the administrator make to enforce HTTPS authentication"? (Choose two >

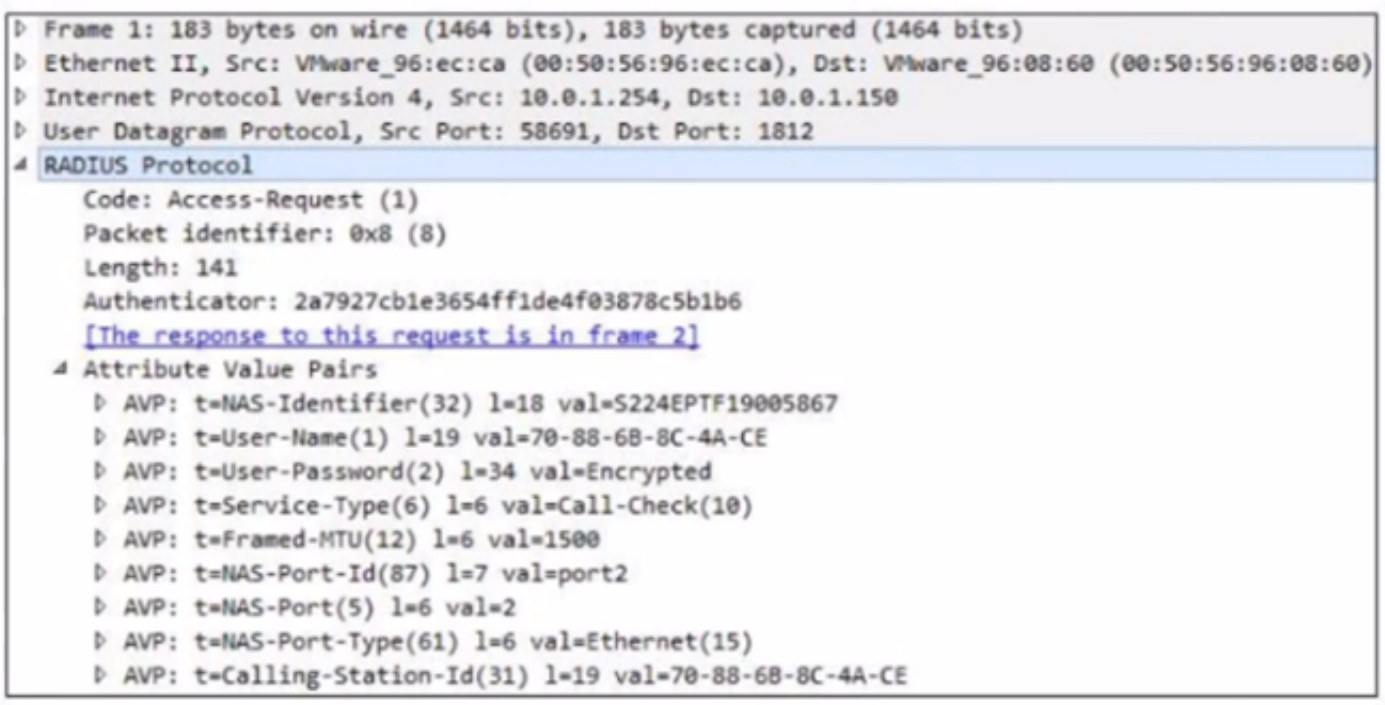
A. Create a new SSID with the HTTPS captive portal URL
B. Enable HTTP redirect in the user authentication settings
C. Disable HTTP administrative access on the guest SSID to enforce HTTPS connection
D. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator

Answer: BD

Explanation:
According to the FortiGate Administration Guide, “To enable HTTPS authentication, you must enable HTTP redirect in the user authentication settings. This redirects HTTP requests to HTTPS. You must also update the captive portal URL to use HTTPS on both FortiGate and FortiAuthenticator.” Therefore, options B and D are true because they describe the changes that the administrator must make to enforce HTTPS authentication for the captive portal. Option A is false because creating a new SSID with the HTTPS captive portal URL is not required, as the existing SSID can be updated with the new URL. Option C is false because disabling HTTP
administrative access on the guest SSID will not enforce HTTPS connection, but rather block HTTP connection.

NEW QUESTION 10
Refer to the exhibit.





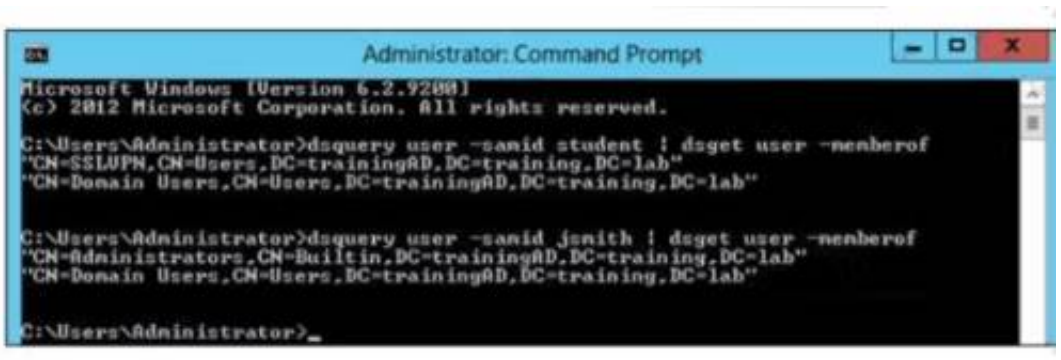
Examine the network diagram and packet capture shown in the exhibit
The packet capture was taken between FortiGate and FortiAuthenticator and shows a RADIUS Access-Request packet sent by FortiSwitch to FortiAuthenticator through FortiGate
Why does the User-Name attribute in the RADIUS Access-Request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



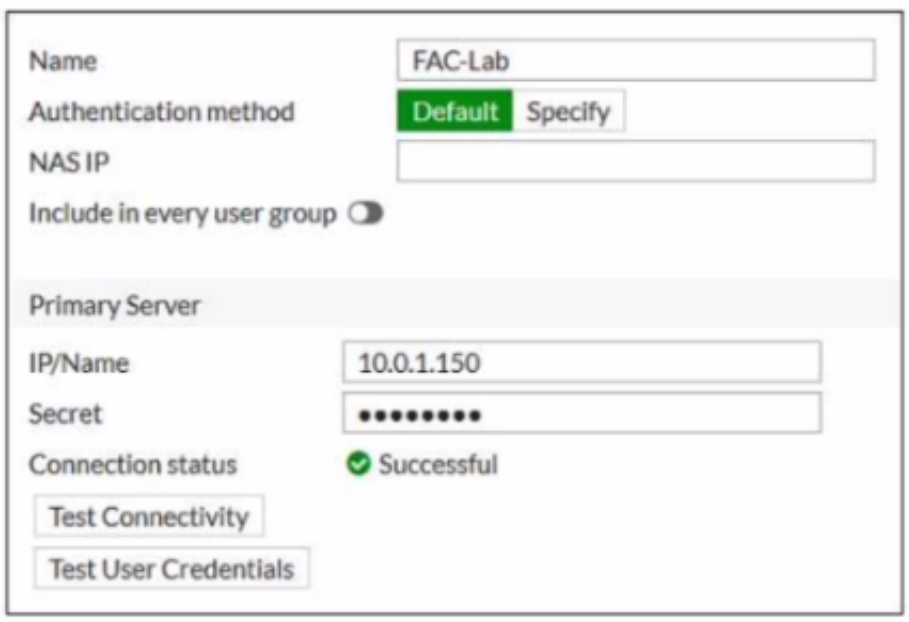
Examine the FortiGate user group configuration and the Windows AD LDAP group membership information shown in the exhibit
FortiGate is configured to authenticate SSL VPN users against Windows AD using LDAP The administrator configured the SSL VPN user group for SSL VPN users However the administrator 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
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 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 21
.....

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