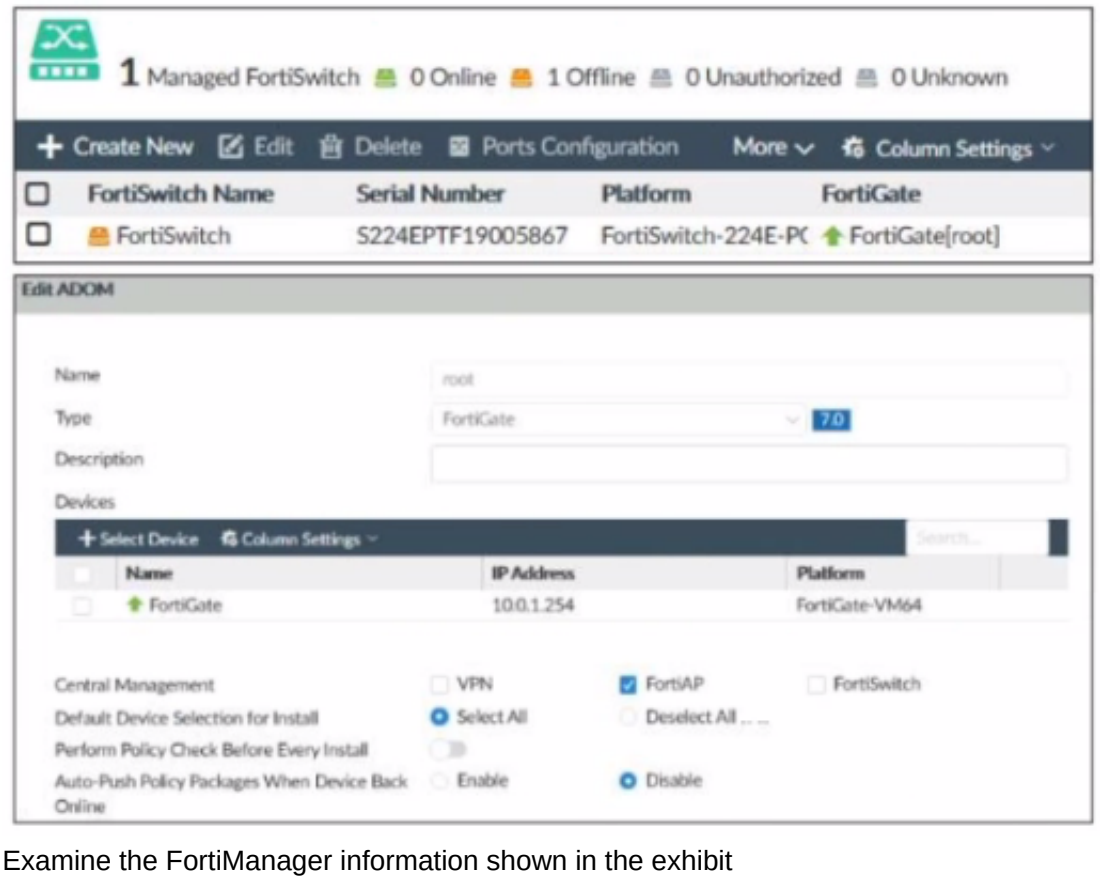
Exam Questions NSE7_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0

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

NEW QUESTION 1
Refer to the exhibit.



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

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

Answer: CD

Explanation:
According to the FortiManager Administration Guide, “Central management mode allows you to manage all FortiSwitch devices from a single interface on the FortiManager device.” Therefore, option C is true because the exhibit shows that the FortiSwitch manager is enabled and the FortiSwitch device is managed by the FortiManager device. Option D is also true because the exhibit shows that the FortiSwitch device status is offline, which means that it is not reachable by the FortiManager device, but it is authorized, which means that it has been added to the FortiManager device. Option A is false because per-device management mode allows you to manage each FortiSwitch device individually from its own web-based manager or CLI, which is not the case in the exhibit. Option B is false because the FortiSwitch device is authorized, as explained above.

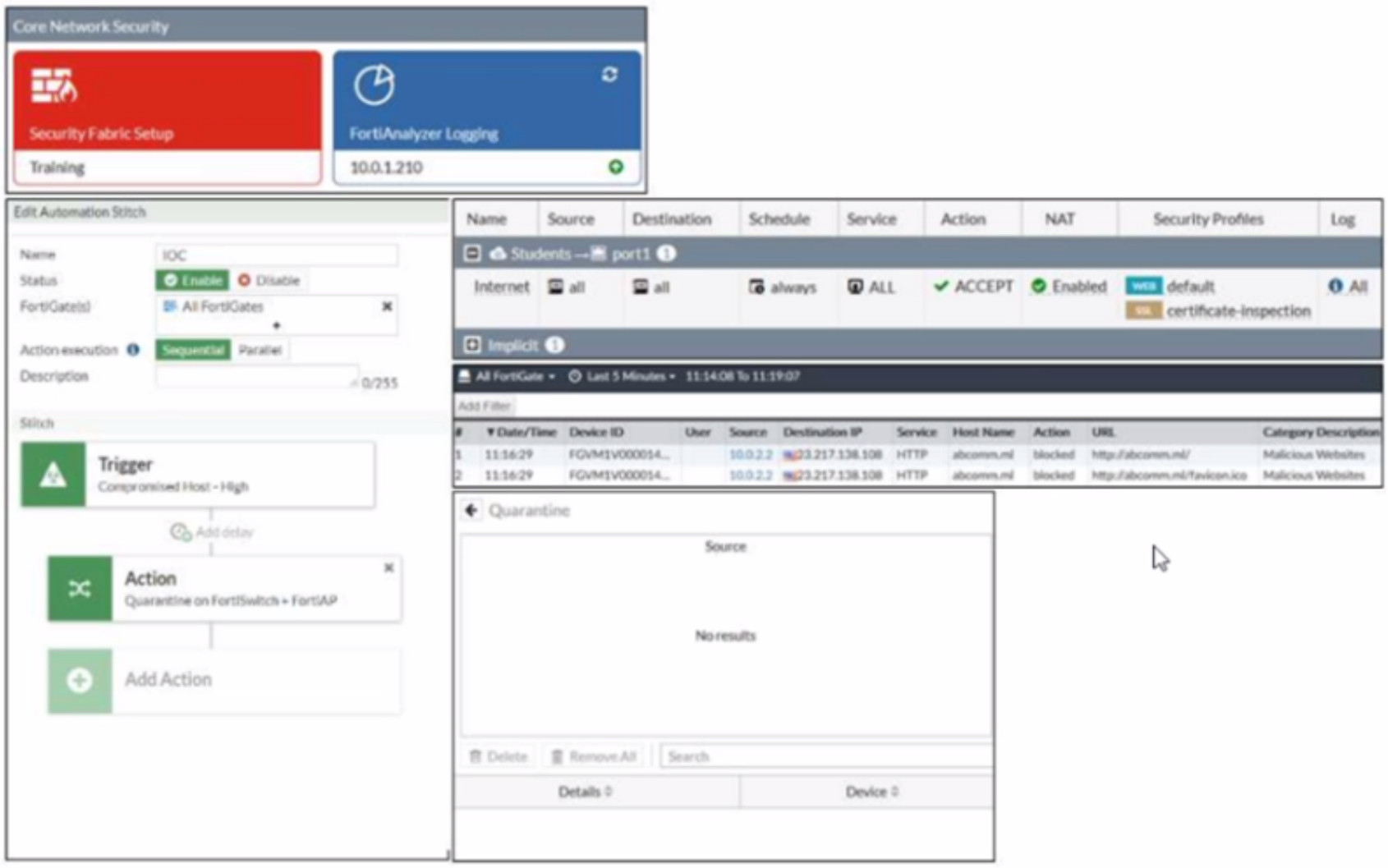
NEW QUESTION 2
Which two pieces of information can the diagnose test authserver ldap command provide? (Choose two.)

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

Answer: BC

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.

NEW QUESTION 3
Refer to the exhibit.



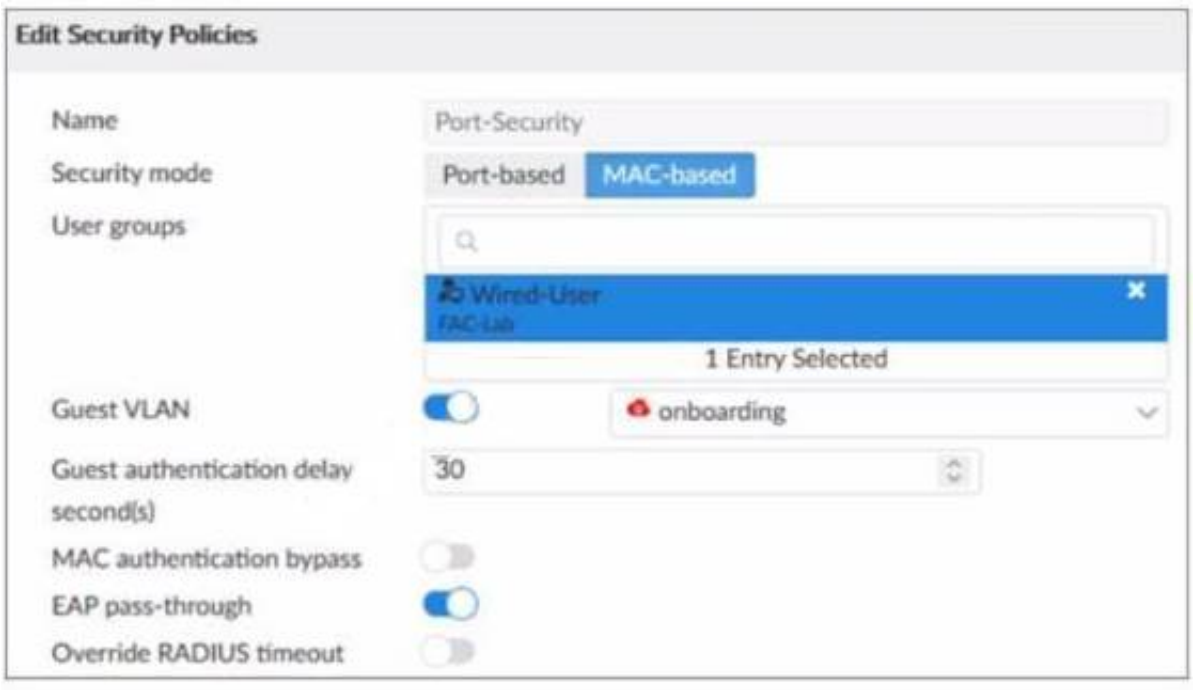
Examine the FortiGate configuration FortiAnalyzer logs and FortiGate widget shown in the exhibit
An administrator is testing the Security Fabric quarantine automation The administrator added FortiAnalyzer to the Security Fabric and configured an automation stitch to automatically quarantine compromised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

Answer: BD

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.

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
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
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.

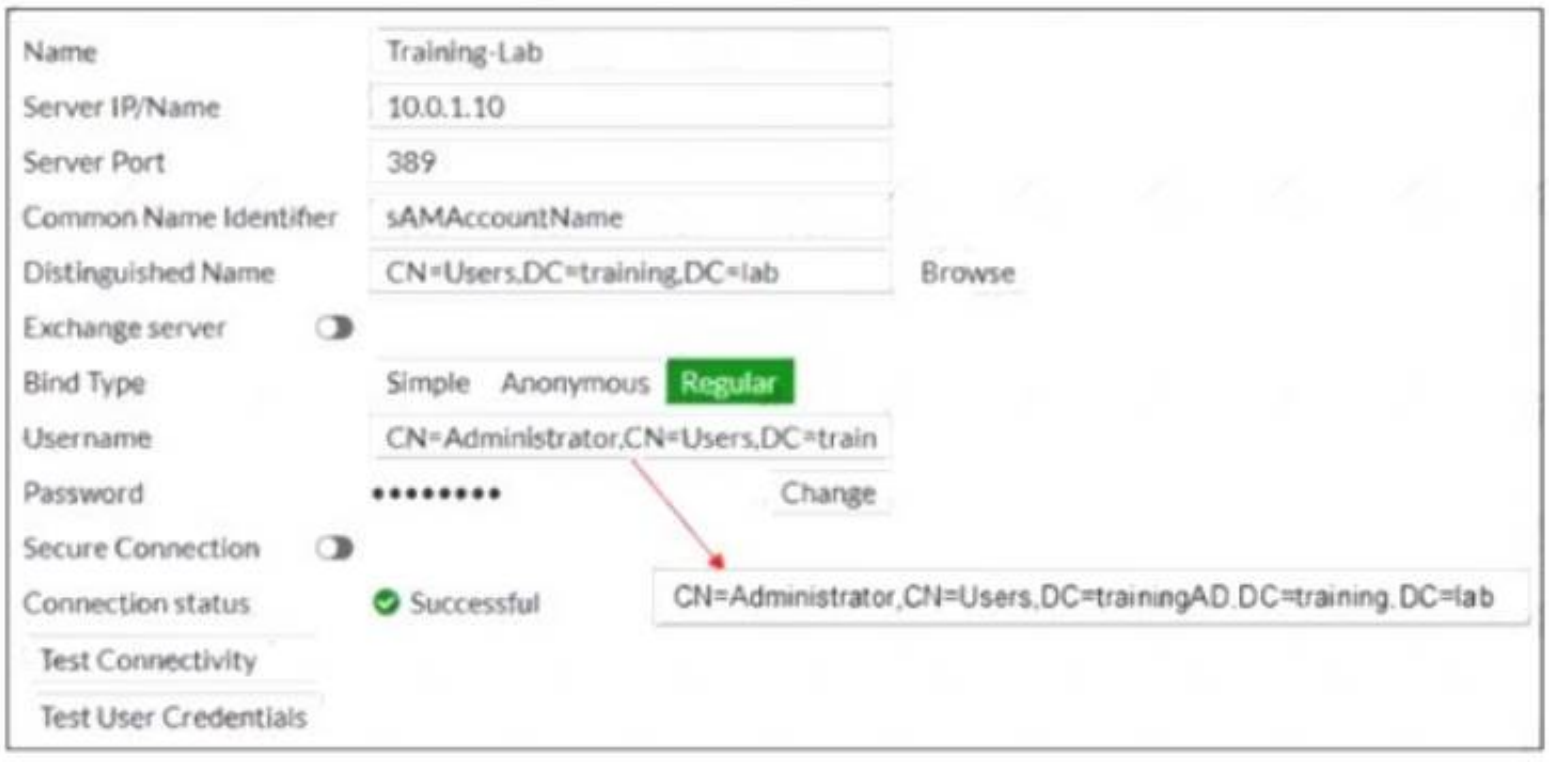
NEW QUESTION 7
You are investigating a report of poor wireless performance in a network that you manage. The issue is related to an AP interface in the 5 GHz range You are monitoring the channel utilization over time.
What is the recommended maximum utilization value that an interface should not exceed?

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.



Examine the LDAP server configuration shown in the exhibit Note that the Username setting has been expanded to display Its full content
On the Windows AD server 10.0.1.10, the administrator used dsquery. which returned the following output:

```
>dsquery user -samid student
"CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab"
```

According to the output which FortiGate LDAP setting is configured incorrectly''

A. Common Name Identifier
B. Bind Type
C. Distinguished Name
D. Username

Answer: C

Explanation:
According to the exhibits, the LDAP server configuration on FortiGate has the Distinguished Name set to “dc=training,dc=lab”. However, according to the output of the dsquery command on the Windows AD server, the Distinguished Name of the domain should be “dc=trainingAD,dc=training,dc=lab”. Therefore, option C is true because the Distinguished Name on FortiGate is configured incorrectly and does not match the actual Distinguished Name of the domain. Option A is false because the Common Name Identifier on FortiGate is configured correctly as “cn”. Option B is false because the Bind Type on FortiGate is configured correctly as “Regular”. Option D is false because the Username on FortiGate is configured correctly as “cn=admin,cn=users,dc=trainingAD,dc=training,dc=lab”.

NEW QUESTION 9
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 10
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.

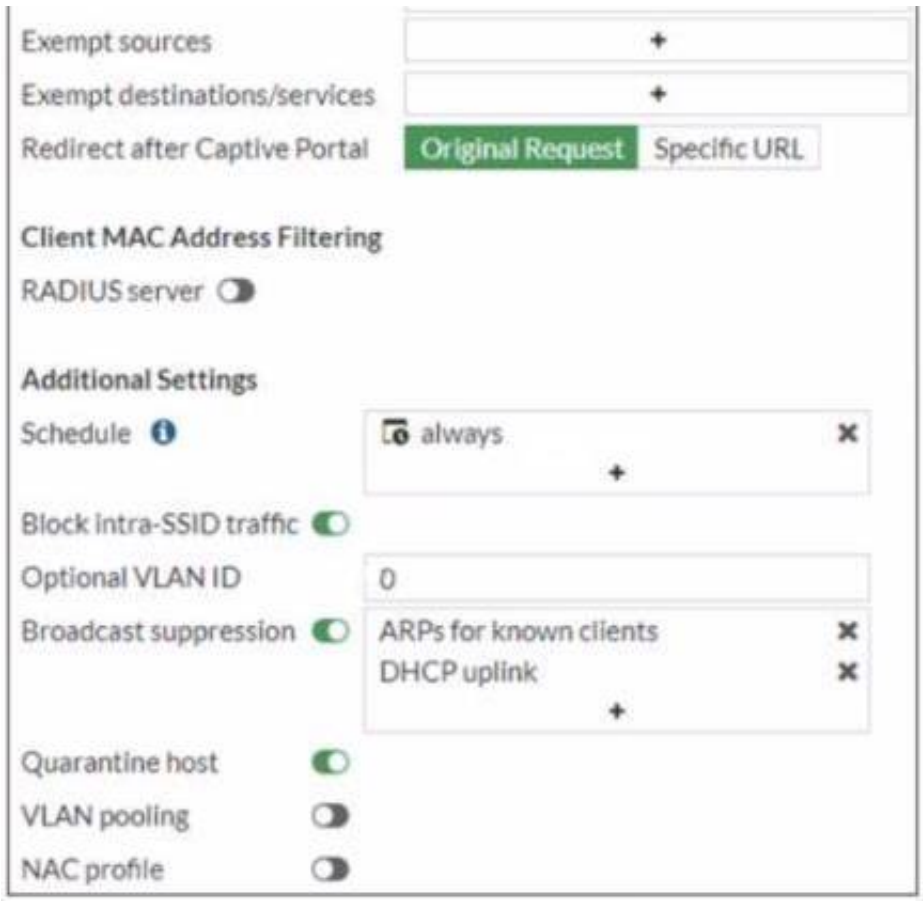
NEW QUESTION 10
An administrator has configured an SSID in bridge mode for corporate employees All APs are online and provisioned using default AP profiles Employees are unable to locate the SSID to conned
Which two configurations can the administrator verify? (Choose two)

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 14
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 17
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 20

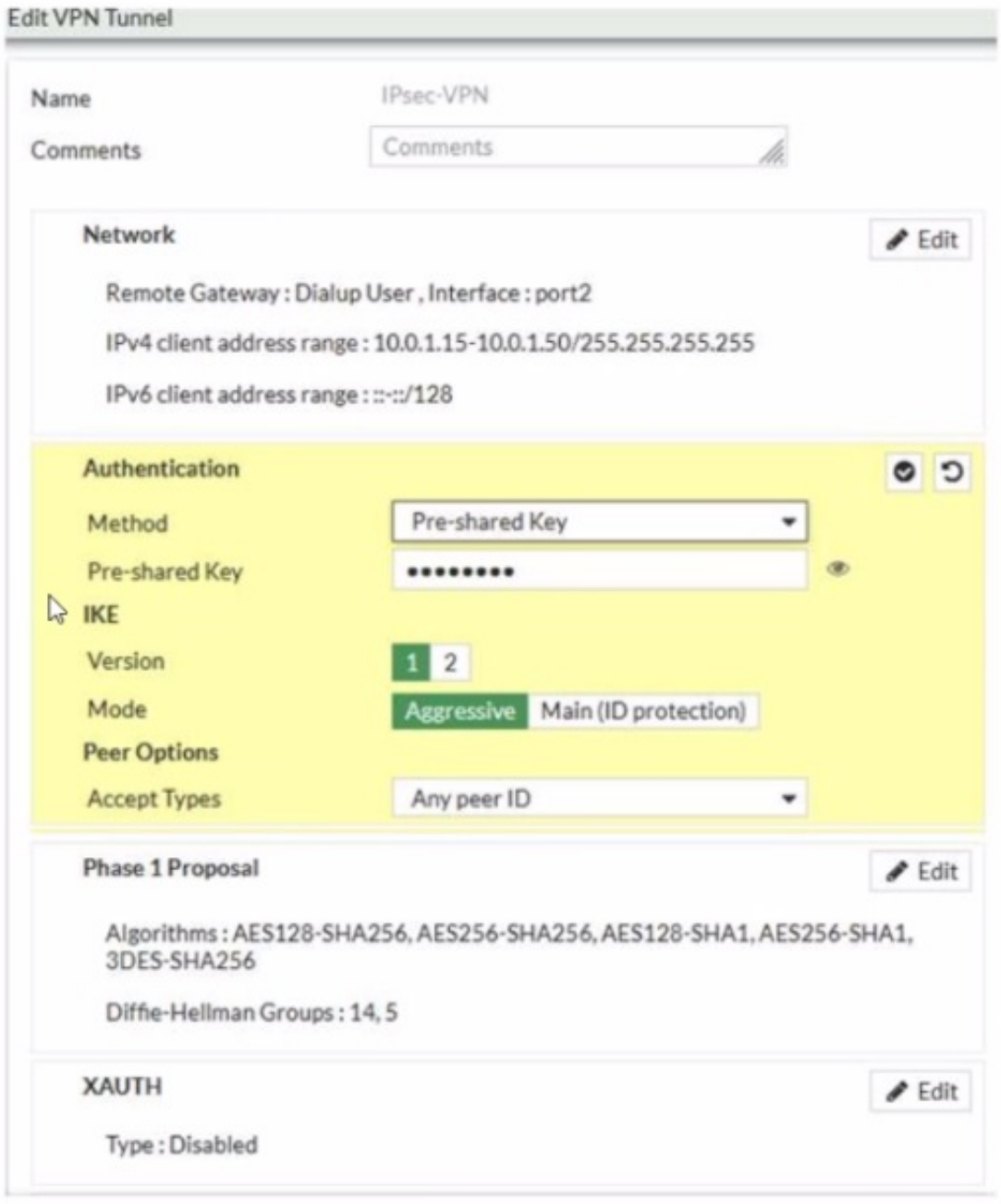
A wireless network in a school provides guest access using a captive portal to allow unregistered users to self-register and access the network The administrator is requested to update the existing configuration to provide captive portal authentication through a secure connection (HTTPS)
Which two changes 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 22
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

Answer: BDE

Explanation:
According to the FortiGate Administration Guide, “To use certificate-based authentication, you must configure the following settings on both peers: Select Signature as the authentication method and select a certificate to use for authentication. Import the CA certificate that issued the peer’s certificate. Enable XAUTH on the phase 1 configuration.” Therefore, options B, D, and E are true because they describe the configuration changes that must be made on FortiGate to perform certificate-based authentication for the IPsec VPN user. Option A is false because creating a PKI user for the IPsec VPN user is not required, as the user certificate can be verified by the CA certificate. Option C is false because changing the IKE mode to Main (ID protection) is not required, as the IKE mode can be either Main or Aggressive for certificate-based authentication.

NEW QUESTION 23
Refer to the exhibit.

```
FortiGate # diagnose test authserver radius FAC-Lab mschap2 student password
[1909] handle_req-Rcvd auth req 1288058912 for student in FAC-Lab opt=0000001d prot=4
[466] __compose_group_list_from_req-Group 'FAC-Lab', type 1
[617] fnbamd_pop3_start-student
[505] __fnbamd_cfg_get_radius_list_by_server-Loading RADIUS server 'FAC-Lab'
[342] fnbamd_create_radius_socket-Opened radius socket 13
[342] fnbamd_create_radius_socket-Opened radius socket 14
[1392] fnbamd_radius_auth_send-Compose RADIUS request
[1352] fnbamd_rad_dns_cb-10.0.1.150->10.0.1.150
[1330] __fnbamd_rad_send-Sent radius req to server 'FAC-Lab': fd=13, IP=10.0.1.150(10.0.1.150:1812) code=1 id=2 len=180 us
er="student" using MS-CHAPv2
[320] radius_server_auth-Timer of rad 'FAC-Lab' is added
  33] create_auth_session-Total 1 server(s) to try
  359] fnbamd_auth_handle_radius_result-Timer of rad 'FAC-Lab' is deleted
  800] fnbamd_radius_auth_validate_pkt-RADIUS resp code 2
[320] extract_success_vsas-FORTINET attr, type 1, val SSLVPN
[1661] __radius_decode_mppe_key-Key len after decode 16

[1661] __radius_decode_mppe_key-Key len after decode 16

[1385] fnbamd_auth_handle_radius_result-->Result for radius svr 'FAC-Lab' 10.0.1.150(1) is 0
[266] find_matched_usr_grps-Skipped group matching
[217] fnbamd_comm_send_result-Sending result 0 (nid 0) for req 1288058912, len=2156
authenticate 'student' against 'mschap2' succeeded, server=primary assigned_rad_session_id=1288058912 session_timeout=0 se
cs idle_timeout=0 secs!
Group membership(s) - SSLVPN
```

Examine the debug output shown in the exhibit
Which two statements about the RADIUS debug output are true" (Choose two)

A. The user student belongs to the SSLVPN group
B. User authentication failed
C. The RADIUS server sent a vendor-specific attribute in the RADIUS response
D. User authentication succeeded using MSCHAP

Answer: AD

Explanation:
According to the exhibit, the debug output shows a RADIUS debug output from FortiGate. The output shows that FortiGate sent a RADIUS Access-Request packet to FortiAuthenticator with the username student and received a RADIUS Access-Accept packet from FortiAuthenticator with a Class attribute containing SSLVPN. Therefore, option A is true because it indicates that the user student belongs to the SSLVPN group on FortiAuthenticator. The output also shows that FortiGate used MSCHAP as the authentication method and received a MS-MPPE-Send-Key and a MS-MPPE-Recv-Key from FortiAuthenticator. Therefore, option D is true because it indicates that user authentication succeeded using MSCHAP. Option B is false because user authentication did not fail, but rather succeeded. Option C is false because FortiAuthenticator did not send a vendor-specific attribute in the RADIUS response, but rather standard attributes defined by RFCs.

NEW QUESTION 28
.....

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