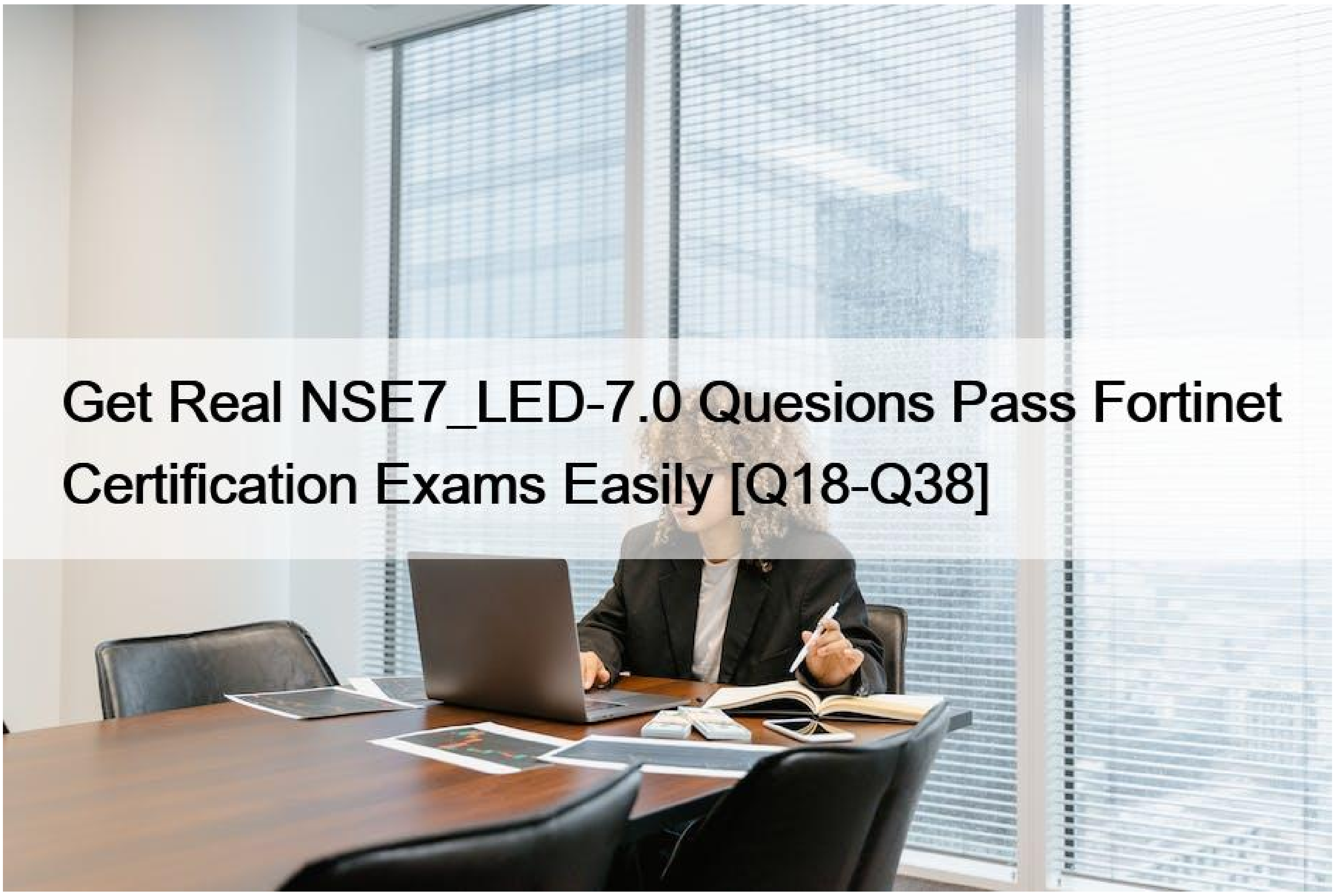
Get Real NSE7_LED-7.0 Quesions Pass Fortinet Certification Exams Easily [Q18-Q38



Get Real NSE7_LED-7.0 Quesions Pass Fortinet Certification Exams Easily
NSE7_LED-7.0 Dumps are Available for Instant Access

One of Fortinet's certification programs is the Fortinet Network Security Expert (NSE) program. The NSE program is a comprehensive training and certification program that covers all aspects of Fortinet's cybersecurity solutions. It is designed to help IT professionals develop the skills and knowledge they need to design, deploy, and manage Fortinet's products effectively. The program has several levels, and the highest level is the NSE7 certification.

Fortinet NSE7_LED-7.0 is a certification exam designed for IT professionals who want to validate their knowledge and expertise in Fortinet NSE 7 - LAN Edge 7.0. NSE7_LED-7.0 exam is intended for those who have a strong understanding of network security and are familiar with Fortinet's security solutions. NSE7_LED-7.0 exam is a comprehensive assessment that covers a wide range of topics related to LAN Edge 7.0.

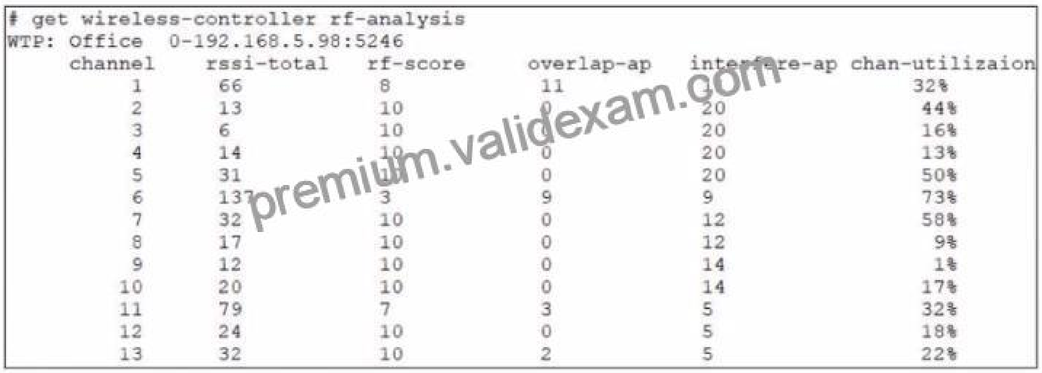
QUESTION 18

Which two statements about the MAC-based 802 1X security mode available on FortiSwitch are true? (Choose two.)
* FortiSwitch authenticates a single device and opens the port to other devices connected to the port
* FortiSwitch authenticates each device connected to the port
* It cannot be used in conjunction with MAC authentication bypass
* FortiSwitch can grant different access levels to each device connected to the port
Explanation

According to the FortiSwitch Administration Guide, &#8220;MAC-based 802.1X security mode allows you to authenticate each device connected to a port using its MAC address as the username and password.&#8221; Therefore, option B is true because it describes the MAC-based 802.1X security mode available on FortiSwitch. Option D is also true because FortiSwitch can grant different access levels to each device connected to the port based on the user group and security policy assigned to them. Option A is false because FortiSwitch does not authenticate a single device and open the port to other devices connected to the port, but rather authenticates each device individually. Option C is false because MAC-based 802.1X security mode can be used in conjunction with MAC authentication bypass (MAB) or EAP pass-through modes, which are fallback options for non-802.1X devices.

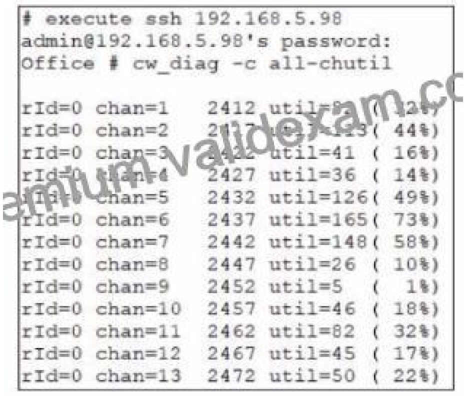
QUESTION 19

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            [illegible]          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?
* Change the AP 2 4 GHz channel to 11
* Change the AP 2 4 GHz channel to 1.
* Change the AP 2 4 GHz channel to 9.
* Change the AP 2 4 GHz channel to 13.
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.

QUESTION 20

Which CLI command should an administrator use to view the certificate verification process in real time?
* diagnose debug application foauthd -1
* diagnose debug application radiusd -1
* diagnose debug application authd -1
* diagnose debug application fnbamd -1
Explanation

According to the FortiOS CLI Reference Guide, &#8220;The diagnose debug application foauthd command enables debugging of certificate verification process in real time.&#8221; 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.

QUESTION 21

Which two statements about MAC address quarantine by redirect mode are true? (Choose two)
* The quarantined device is moved to the quarantine VLAN
* The device MACaddress is added to the Quarantined Devices firewall address group
* It is the default mode for MAC address quarantine
* The quarantined device is kept in the current VLAN
Explanation

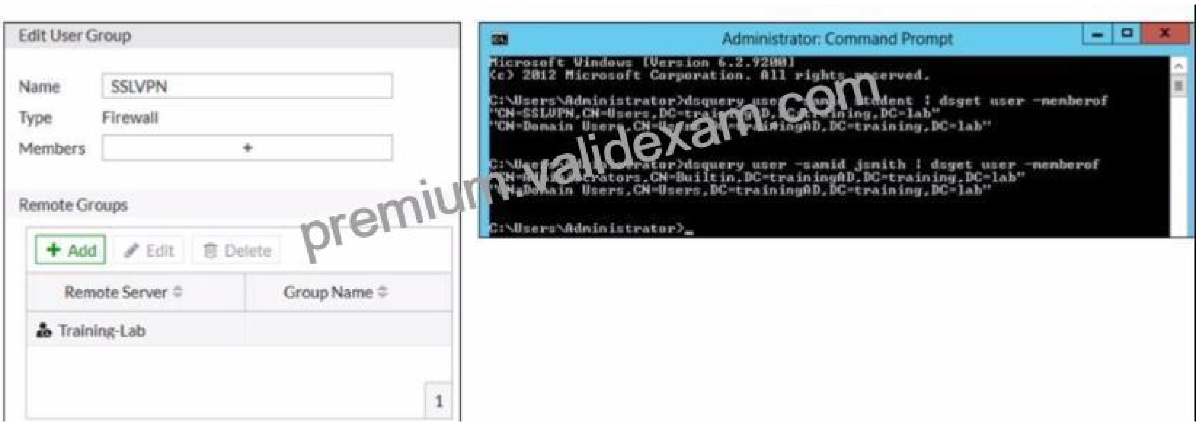
According to the FortiGate Administration Guide, &#8220;MAC address quarantine by redirect mode allows you to quarantine devices by adding their MAC addresses to a firewall address group called Quarantined Devices.

The quarantined devices are kept in their current VLANs, but their traffic is redirected to a quarantine portal.&#8221; 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

QUESTION 22

Refer to the exhibit.



Edit User Group

Name: SSLVPN
Type: Firewall
Members: +

Remote Groups

Remote Server	Group Name
Training-Lab	

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dsquery user -samid student | dsget user -memberof
"CN=SSLVPN,CN=Users,DC=trainingAD,DC=training,DC=lab"
"CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab"

C:\Users\Administrator>dsquery user -samid jsmith | dsget user -memberof
"CN=Administrators,CN=Builtin,DC=trainingAD,DC=training,DC=lab"
"CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab"

C:\Users\Administrator>_
```

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?

- In the SSL VPN user group configuration set Group Nam to CN-SSLVPN, CN=&#8221;users, DC-trainingAD, DC-training, DC-lab
- In the SSL VPN user group configuration, change Name to cn=sslvpn, CN=users, DC=trainingAD, Detraining, DC-lab.
- In the SSL VPN user group configuration set Group Name to ::;=Domain users.CN-Users/DC=trainingAD, DC-training, DC=lab.
- In the SSL VPN user group configuration change Type to Fortinet Single Sign-On (FSSO)

Explanation

According to the FortiGate Administration Guide, &#8220;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.&#8221; 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.

QUESTION 23

You are setting up an SSID (VAP) to perform RADlUS-authenticated dynamic VLAN allocation Which three RADIUS attributes must be supplied by the RADIUS server to enable successful VLAN allocation&#8221; (Choose three.)

- Tunnel-Private-Group-ID

* Tunnel-Pvt-Group-ID
* Tunnel-Preference
* Tunnel-Type
* Tunnel-Medium-Type

Explanation

According to the FortiAP Configuration Guide, &#8220;To perform RADIUS-authenticated dynamic VLAN allocation, the RADIUS server must supply the following RADIUS attributes: Tunnel-Private-Group-ID, which specifies the VLAN ID to assign to the user. Tunnel-Type, which specifies the tunneling protocol used for the VLAN. The value must be 13 (VLAN). Tunnel-Medium-Type, which specifies the transport medium used for the VLAN. The value must be 6 (802). Therefore, options A, D, and E are true because they describe the RADIUS attributes that must be supplied by the RADIUS server to enable successful VLAN allocation.

Option B is false because Tunnel-Pvt-Group-ID is not a valid RADIUS attribute name, but rather a typo for Tunnel-Private-Group-ID. Option C is false because Tunnel-Preference is not a required RADIUS attribute for dynamic VLAN allocation, but rather an optional attribute that specifies the priority of the VLAN.

QUESTION 24

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?

* Access VLAN is enabled on the VLAN
* The native VLAN configured on the ports is incorrect
* The FortiSwitch MAC address table is missing entries
* The FortiGate ARP table is missing entries

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.

QUESTION 25

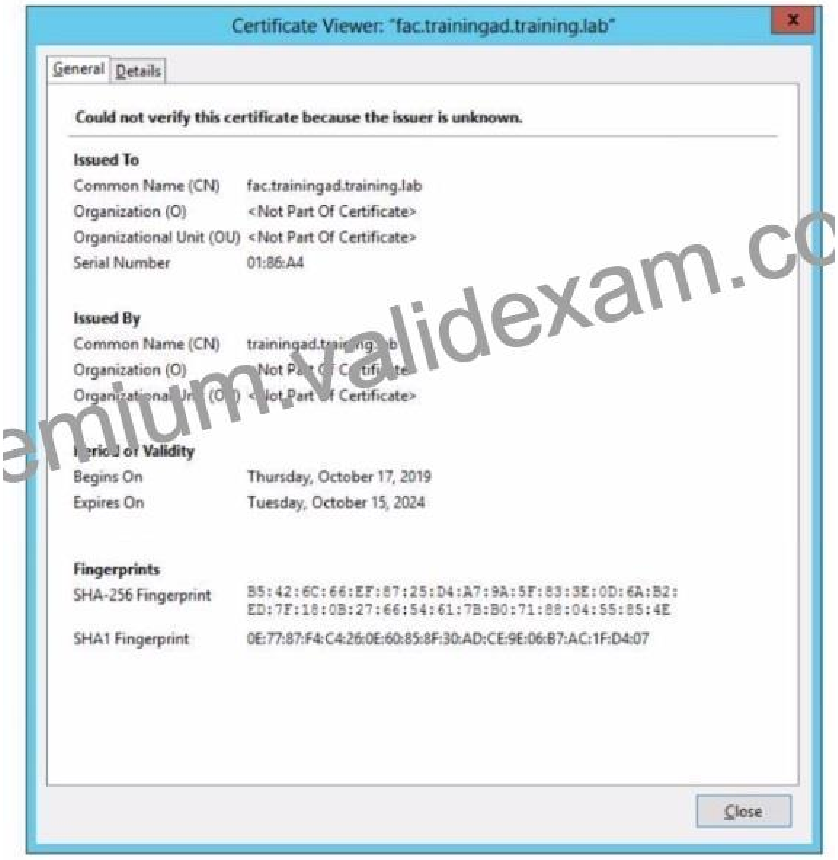
Where can FortiGate learn the FortiManager IP address or FQDN for zero-touch provisioning&#8217;?

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

Explanation

According to the FortiGate Administration Guide, &#8220;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.&#8221; 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.

QUESTION 26



Certificate Viewer: "fac.trainingad.training.lab"

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN) fac.trainingad.training.lab
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 01:86:A4

Issued By

Common Name (CN) trainingad.training.lab
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>

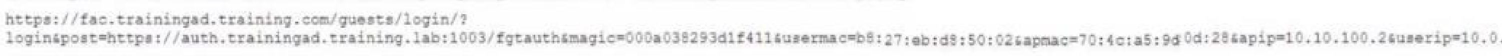
Period of Validity

Begins On Thursday, October 17, 2019
Expires On Tuesday, October 15, 2024

Fingerprints

SHA-256 Fingerprint B5:42:6C:66:EF:87:25:D4:A7:9A:5F:83:3E:0D:6A:B2:ED:7F:18:0B:27:66:54:61:7B:B0:71:88:04:55:85:4E
SHA1 Fingerprint 0E:77:87:F4:C4:26:0E:60:85:8F:30:AD:CE:9E:06:B7:AC:1F:D4:07

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



```
https://fac.trainingad.training.com/guests/login/?
login&post=https://auth.trainingad.training.lab:1003/fgtauth&magic=000a038293d1f411&usermac=b8:27:eb:d8:50:02&apmac=70:4c:a5:9d:0d:28&apip=10.10.100.2&userip=10.0.
```

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

* The external server FQDN is incorrect
* The wireless user&#8217;s browser is missing a CA certificate

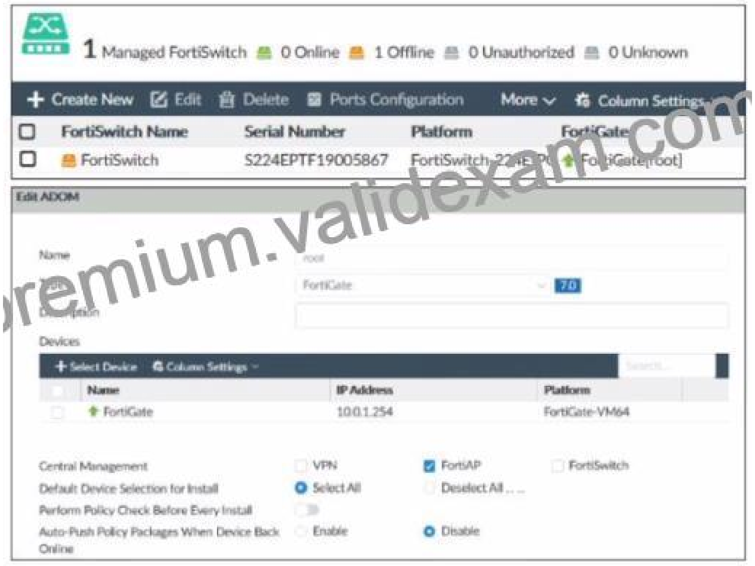
* The FortiGate authentication interface address is using HTTPS
* The user address is not in DDNS form
Explanation

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

Therefore, option A is true because the external server FQDN is incorrect, which means that it does not match the common name or subject alternative name of the server certificate. Option B is also true because the wireless user&#8217;s browser is missing a CA certificate, which means that it does not have the root or intermediate certificate that issued the server certificate. Option C is false because the FortiGate authentication interface address is using HTTPS, which is a secure protocol that encrypts the communication between the browser and the server. Option D is false because the user address is not in DDNS form, which is not related to the certificate error.

QUESTION 27

Refer to the exhibit.



1 Managed FortiSwitch 0 Online 1 Offline 0 Unauthorized 0 Unknown

□	FortiSwitch Name	Serial Number	Platform	FortiGate
□	FortiSwitch	S224EPTF19005867	FortiSwitch-224E-POE	FortiGate[root]

Edit ADOM

Name: root
Type: FortiGate 7.0
Description:
Devices

□	Name	IP Address	Platform
□	FortiGate	10.0.1.254	FortiGate-VM64

Central Management: □ VPN ☑ FortiAP □ FortiSwitch
Default Device Selection for Install: ● Select All ○ Deselect All ...
Perform Policy Check Before Every Install:
Auto-Push Policy Packages When Device Back Online: ○ Enable ● Disable

Examine the FortiManager information shown in the exhibit

Which two statements about the FortiManager status are true&#8221; (Choose two)
* FortiSwitch manager is working in per-device management mode
* FortiSwitch is not authorized
* FortiSwitch manager is working in central management mode
* FortiSwitch is authorized and offline
Explanation

According to the FortiManager Administration Guide, &#8220;Central management mode allows you to manage all FortiSwitch devices from a single interface on the FortiManager device.&#8221; Therefore, option C is true because the exhibit shows that the FortiSwitch manager is enabled and the FortiSwitch device is managed by the FortiManager device. Option D is also true because the exhibit shows that the FortiSwitch device status is offline, which means that it is not reachable by the FortiManager device, but it is authorized, which means that it has been added to the FortiManager device. Option A is false because per-device management mode allows you to manage each FortiSwitch device individually from its own web-based manager or CLI, which is not the case in the exhibit. Option B is false because the FortiSwitch device is authorized, as explained above.

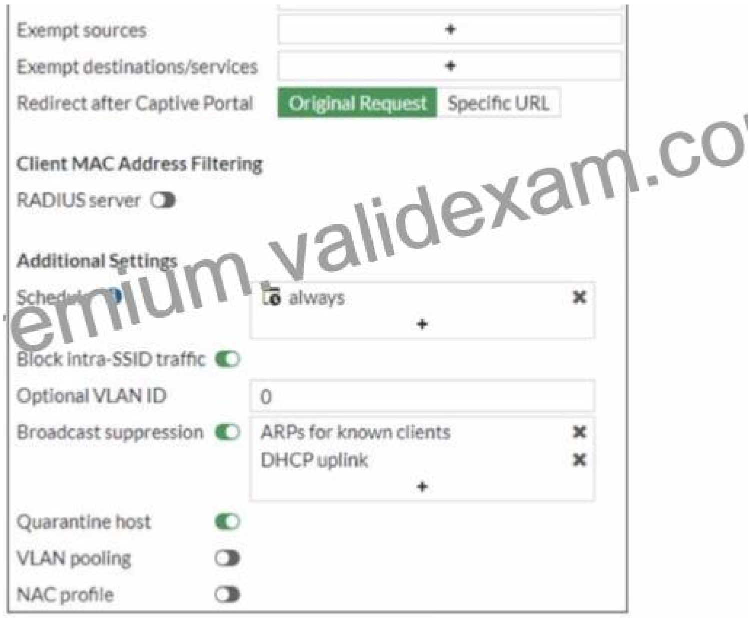
QUESTION 28

You are configuring a FortiGate wireless network to support automated wireless client quarantine using IOC Which two configurations must you put in place for a wireless client to be quarantined successfully? (Choose two)
* Configure the wireless network to be in tunnel mode
* Configure the FortiGate device in the Security Fabric with a FortiAnalyzer device
* Configure a firewall policy to allow communication
* Configure the wireless network to be in bridge mode
Explanation

According to the FortiGate Administration Guide, &#8220;To enable automated wireless client quarantine using IOC, you must configure the following settings: Configure your wireless network to be in tunnel mode. This allows FortiGate to inspect all wireless traffic and applysecurity policies. Configure your FortiGate device in the Security Fabric with a FortiAnalyzer device. This allows FortiAnalyzer to detect indicators of compromise (IOC) from wireless traffic and send quarantine commands to FortiGate.&#8221; Therefore, options A and B are true because they describe the configurations that must be put in place for a wireless client to be quarantined successfully using IOC. Option C is false because configuring a firewall policy to allow communication is not required, as the default firewall policy for tunnel mode wireless networks is to allow all traffic. Option D is false because configuring the wireless network to be in bridge mode is not supported, as FortiGate cannot inspect or quarantine wireless traffic in bridge mode.

QUESTION 29

Refer to the exhibits.

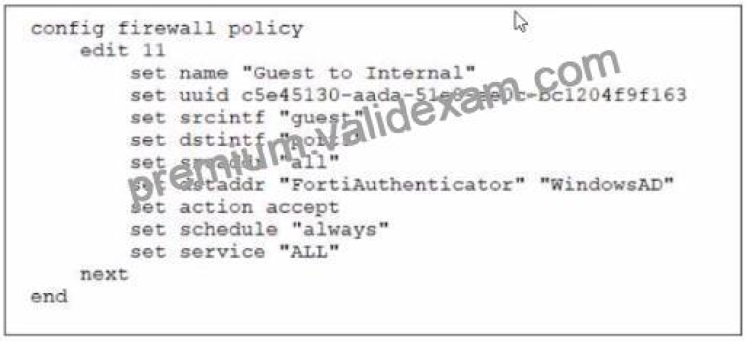


Exempt sources +
Exempt destinations/services +
Redirect after Captive Portal [✓ Original Request] Specific URL

Client MAC Address Filtering
RADIUS server ○

Additional Settings
Schedule ● always ✖ +
Block intra-SSID traffic ●
Optional VLAN ID 0
Broadcast suppression ● ARPs for known clients ✖ DHCP uplink ✖ +
Quarantine host ●
VLAN pooling ○
NAC profile ○

Firewall Policy



```
config firewall policy
    edit 11
        set name "Guest to Internal"
        set uuid c5e45130-aada-51e8-[illegible]-bc1204f9f163
        set srcintf "guest"
        set dstintf "port1"
        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?

* Disable the user group from the SSID configuration
* Enable the captivs-portal-exempt option in the firewall policy with the ID 11.
* Apply a guest.portal user group in the firewall policy with the ID 11.
* Include the wireless client subnet range in the Exempt Source section

Explanation

According to the FortiGate Administration Guide, &#8220;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.&#8221; 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.

QUESTION 30

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

* It displays whether the admin bind user credentials are correct
* It displays whether the user credentials are correct
* It displays the LDAP codes returned by the LDAP server
* It displays the LDAP groups found for the user

Explanation

According to the FortiGate CLI Reference Guide, &#8220;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.&#8221; Therefore, options B and C are true because they describe the information that the diagnose test authserver ldap command can provide. Option A is false because the command does not display whether the admin bind user credentials are correct, but rather whether the user credentials are correct. Option D is false because the command does not display the LDAP groups found for the user, but rather whether the user belongs to any groups that match a firewall policy.

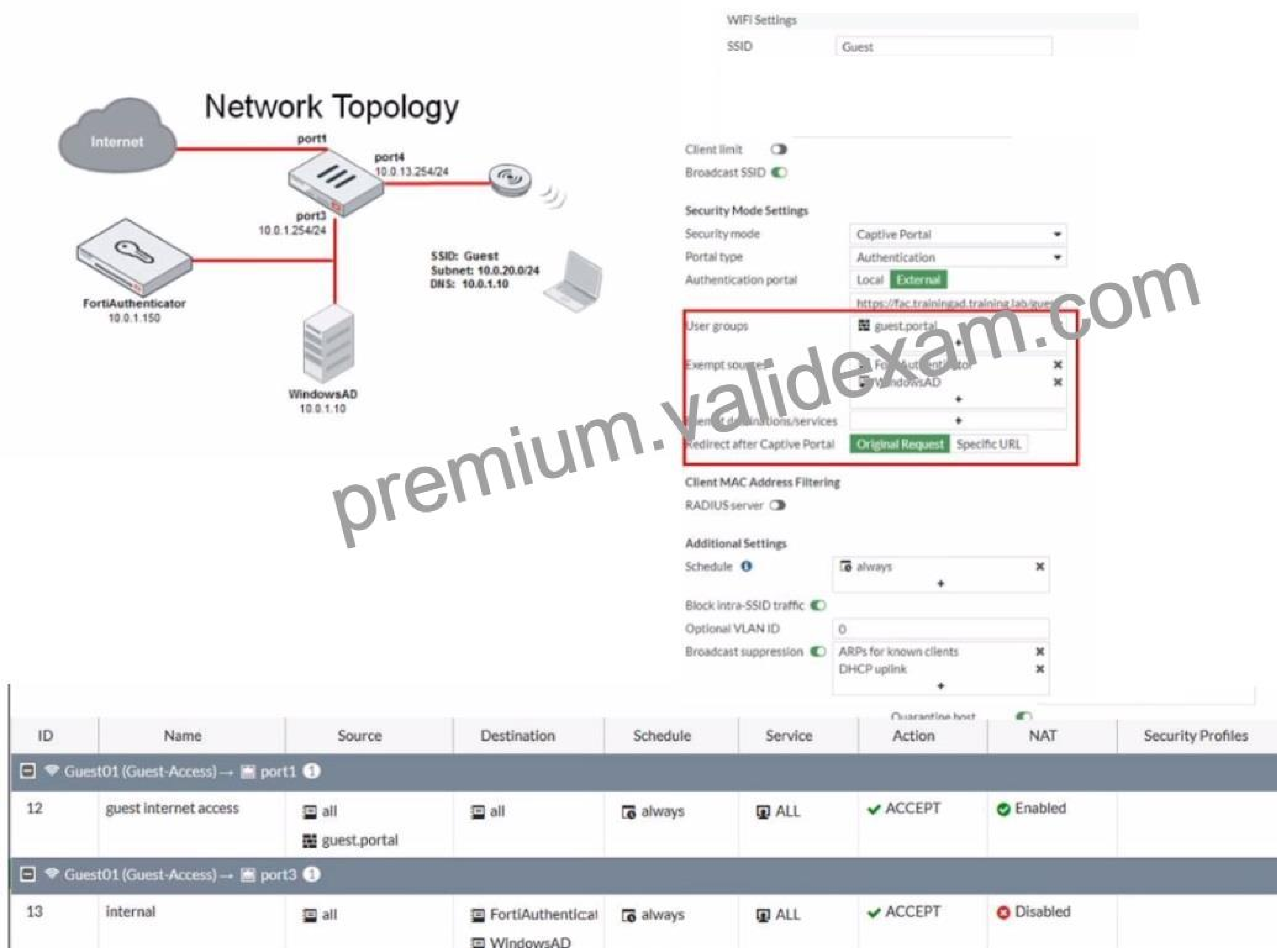
QUESTION 31

Which EAP method requires the use of a digital certificate on both the server end and the client end?
* EAP-TTLS
* PEAP
* EAP-GTC
* EAP-TLS
Explanation

According to the FortiGate Administration Guide, &#8220;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.&#8221; 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.

QUESTION 32

Exhibit.



WIFI Settings
SSID: Guest

Client limit ○
Broadcast SSID ●

Security Mode Settings
Security mode: Captive Portal
Portal type: Authentication
Authentication portal: Local [✓ External]
https://fac.trainingad.training.lab/gues
User groups: guest.portal
Exempt sources: FortiAuthenticator, WindowsAD
Exempt destinations/services
Redirect after Captive Portal: [✓ Original Request] Specific URL

Client MAC Address Filtering
RADIUS server ○

Additional Settings
Schedule: always
Block intra-SSID traffic ●
Optional VLAN ID: 0
Broadcast suppression ●: ARPs for known clients, DHCP uplink
Quarantine host ●

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
Guest01 (Guest-Access) → port1								
12	guest internet access	all guest.portal	all	always	ALL	✓ ACCEPT	✓ Enabled	
Guest01 (Guest-Access) → port3								
13	internal	all	FortiAuthentica WindowsAD	always	ALL	✓ ACCEPT	✗ Disabled	

Refer to the exhibit showing a network topology and SSID settings.

FortiGate is configured to use an external captive portal However wireless users are not able to see the captive portal login page Which configuration change should the administrator make to fix the problem?

* Enable NAT in the firewall policy with the ID 13.
* Add the FortiAuthenticator and WindowsAD address objects as exempt destinations services
* Enable the captive-portal-exempt option in the firewall policy with the ID 12
* Remove the guest.portal user group in the firewall policy with the ID 12

Explanation

According to the exhibit, the network topology and SSID settings show that FortiGate is configured to use an external captive portal hosted on FortiAuthenticator, which is connected to a Windows AD server for user authentication. However, wireless users are not able to see the captive portal login page, which means that they are not redirected to the external captive portal URL. Therefore, option B is true because adding the FortiAuthenticator and WindowsAD address objects as exempt destinations services will allow the wireless users to access the external captive portal URL without being blocked by the firewall policy. Option A is false because enabling NAT in the firewall policy with the ID 13 will not affect the redirection to the external captive portal URL, but rather the source IP address of the wireless traffic. Option C is false because enabling the captive-portal-exempt option in the firewall policy with the ID 12will bypass the captive portal authentication for the wireless users, which is not the desired outcome. Option D is false because removing the guest.portal user group in the firewall policy with the ID 12 will prevent the wireless users from being authenticated by FortiGate, which is required for accessing the external captive portal.

QUESTION 33

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

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

Explanation

According to the FortiAuthenticator Administration Guide2, &#8220;Windows Active Directory domain authentication enables FortiAuthenticator to join a Windows Active Directory domain as a machine entity and proxy authentication requests using Kerberos.&#8221; 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.

Get Instant Access REAL NSE7_LED-7.0 DUMP Pass Your Exam Easily:
https://www.validexam.com/NSE7_LED-7.0-latest-dumps.html]