



Fortinet

Exam Questions NSE7_LED-7.0

Fortinet NSE 7 - LAN Edge 7.0

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

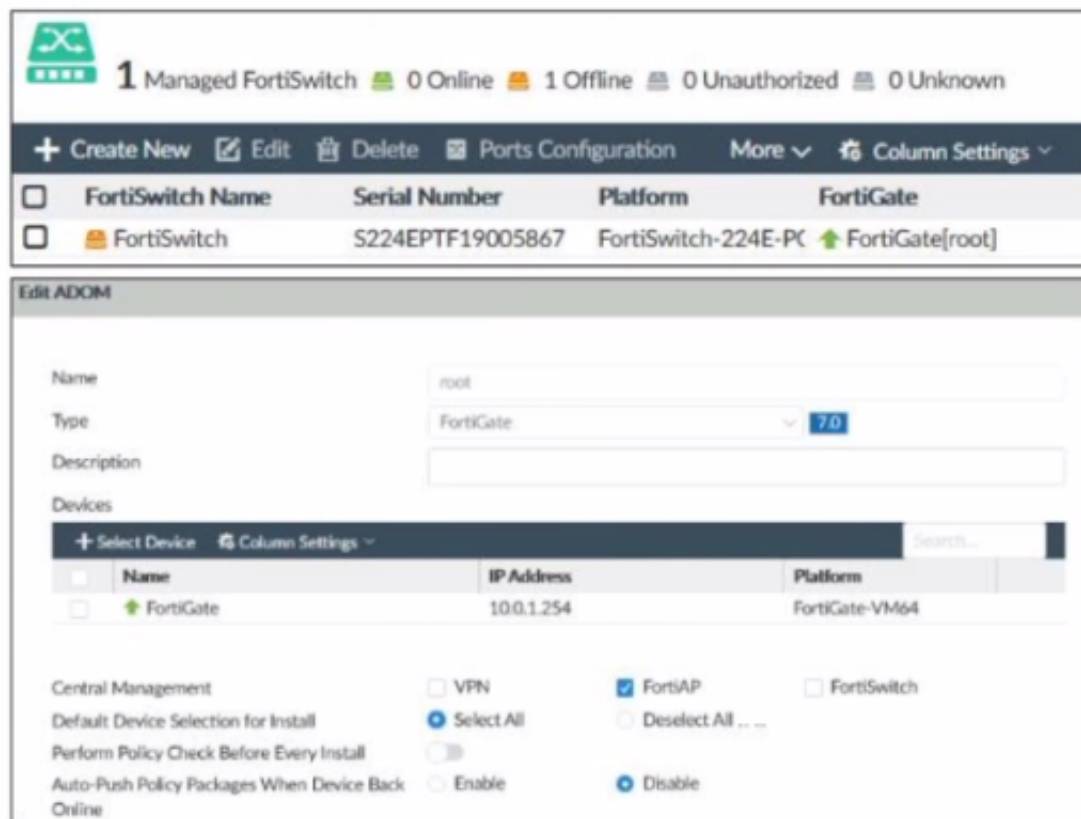
Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

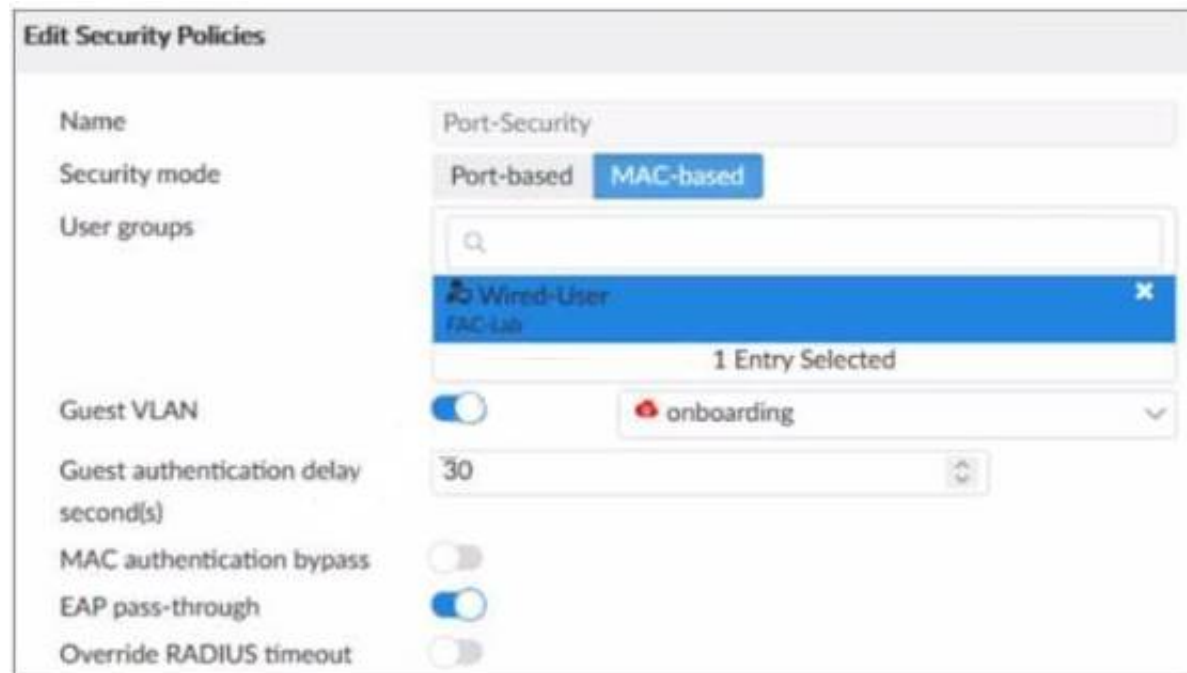
Answer: CD

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

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 3

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 4
Refer to the exhibits.

SSID Profiles

Name	SSID	Traffic Mode	Security Mode	Data
▼ SSIDs (4)				
<input type="checkbox"/>	CompanyPrinters	Corp Printers	Tunnel	WPA2 Personal AES
<input type="checkbox"/>	Employees-Red	employees	Tunnel	WPA2 Enterprise AES
<input type="checkbox"/>	Guest-CorpPort	fortinet-cp	Tunnel	Captive Portal
<input type="checkbox"/>	PSK	PSK	Tunnel	WPA2 Personal AES

AP Profile

Name: FAPU431F-MainCampus

Comments: 0/255

Platform: FAPU431F

Platform Mode: Single 5G Dual 5G

Country/ Region: United States

AP Login Password: Set Leave Unchanged Set Empty

Administrative Access: ☐ HTTPS ☐ SNMP ☐ SSH

Client Load Balancing: ☐ Frequency Handoff ☐ AP Handoff

Bluetooth Profile: None

Radio 1

Mode: Disabled Access Point Dedicated Monitor SAM

WIDS Profile: ☐

Radio Resource Provision: ☐

Band: 5 GHz 802.11ax/ac/n

Channel Width: 20MHz 40MHz 80MHz 160MHz

Short Guard Interval: ☐

Channels:

<input type="checkbox"/> 36	<input type="checkbox"/> 40	<input type="checkbox"/> 44	<input type="checkbox"/> 48	<input type="checkbox"/> 52	<input type="checkbox"/> 56
<input type="checkbox"/> 60	<input type="checkbox"/> 64	<input type="checkbox"/> 100	<input type="checkbox"/> 104	<input type="checkbox"/> 108	<input type="checkbox"/> 112
<input type="checkbox"/> 116	<input type="checkbox"/> 120	<input type="checkbox"/> 124	<input type="checkbox"/> 128	<input type="checkbox"/> 132	<input type="checkbox"/> 136
<input type="checkbox"/> 140	<input type="checkbox"/> 144	<input type="checkbox"/> 149	<input type="checkbox"/> 153	<input type="checkbox"/> 157	<input type="checkbox"/> 161

TX Power Control: Auto Manual

TX Power: 10 17 dBm

SSIDs: Tunnel Bridge Manual

Monitor Channel Utilization: ☒

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 5
Refer to the exhibits.

Exempt sources	<input type="text"/>	+
Exempt destinations/services	<input type="text"/>	+
Redirect after Captive Portal	<input checked="" type="radio"/> Original Request	<input type="radio"/> Specific URL
Client MAC Address Filtering		
RADIUS server	<input type="checkbox"/>	
Additional Settings		
Schedule	<input checked="" type="radio"/> always	+
Block intra-SSID traffic	<input checked="" type="checkbox"/>	
Optional VLAN ID	<input type="text" value="0"/>	
Broadcast suppression	<input checked="" type="checkbox"/>	+
	ARPs for known clients	×
	DHCP uplink	×
Quarantine host	<input checked="" type="checkbox"/>	
VLAN pooling	<input type="checkbox"/>	
NAC profile	<input type="checkbox"/>	

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 captive-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 6

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 Guide, "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 because FortiGate does not measure the signal strength of the weakest associated client, but rather the FortiAP does.

NEW QUESTION 7

Which two statements about the MAC-based 802.1X security mode available on FortiSwitch are true? (Choose two.)

- A. FortiSwitch authenticates a single device and opens the port to other devices connected to the port
- B. FortiSwitch authenticates each device connected to the port
- C. It cannot be used in conjunction with MAC authentication bypass
- D. FortiSwitch can grant different access levels to each device connected to the port

Answer: BD

Explanation:

According to the FortiSwitch Administration Guide, "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." 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.

NEW QUESTION 8

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 9

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

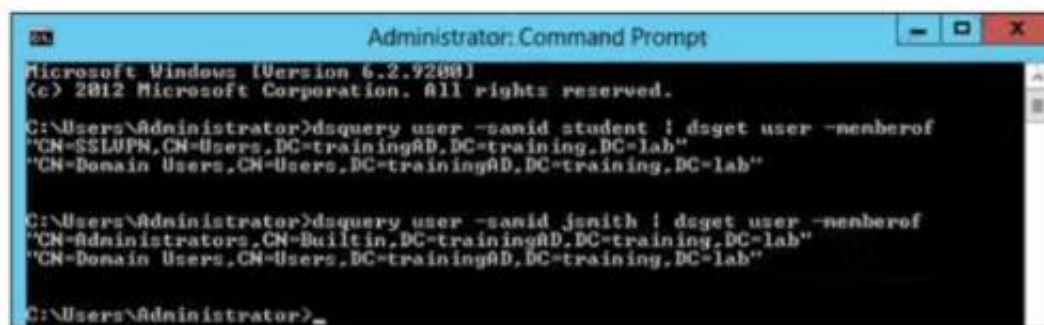
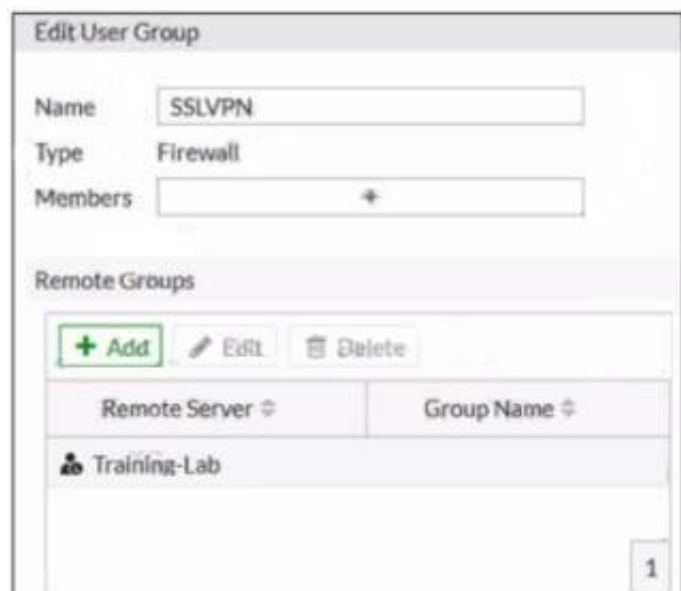
Answer: A

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 10

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 jsmith 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 Name 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)

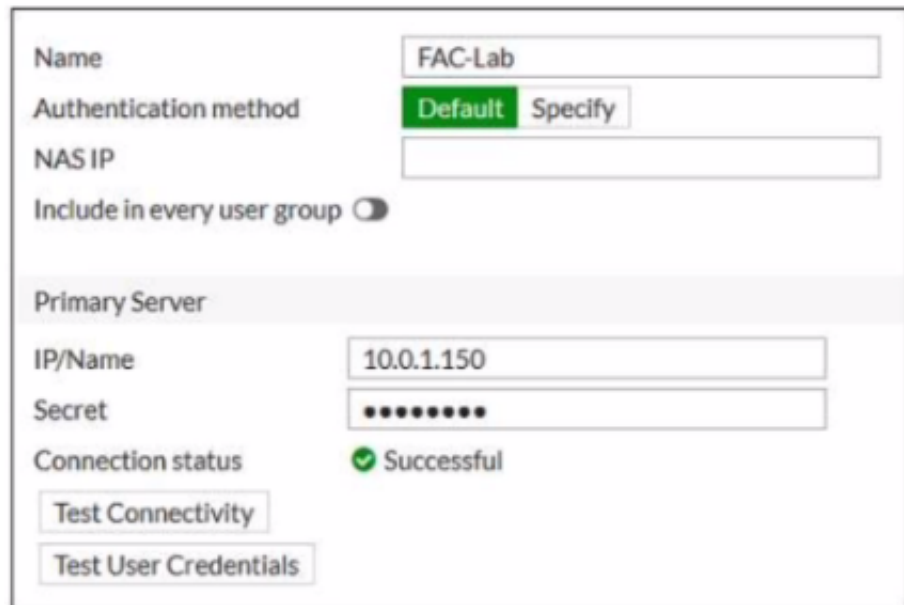
Answer: A

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 10

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 13

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)

- A. Configure the wireless network to be in tunnel mode
 B. Configure the FortiGate device in the Security Fabric with a FortiAnalyzer device
 C. Configure a firewall policy to allow communication
 D. Configure the wireless network to be in bridge mode

Answer: AB

Explanation:

According to the FortiGate Administration Guide, "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 apply security 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." 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.

NEW QUESTION 14

.....

Relate Links

100% Pass Your NSE7_LED-7.0 Exam with Exambible Prep Materials

https://www.exambible.com/NSE7_LED-7.0-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>