# NSE7_SAC-6.2$^{Q\&As}$

Fortinet NSE 7 - Secure Access 6.2

## Pass Fortinet NSE7_SAC-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.geekcert.com/nse7_sac-6-2.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

**QUESTION 1**

Which step can be taken to ensure that only FortiAP devices receive IP addresses from a DHCP server on FortiGate?

A. Change the interface addressing mode to FortiAP devices.

B. Create a reservation list in the DHCP server settings.

C. Configure a VCI string value of FortiAP in the DHCP server settings.

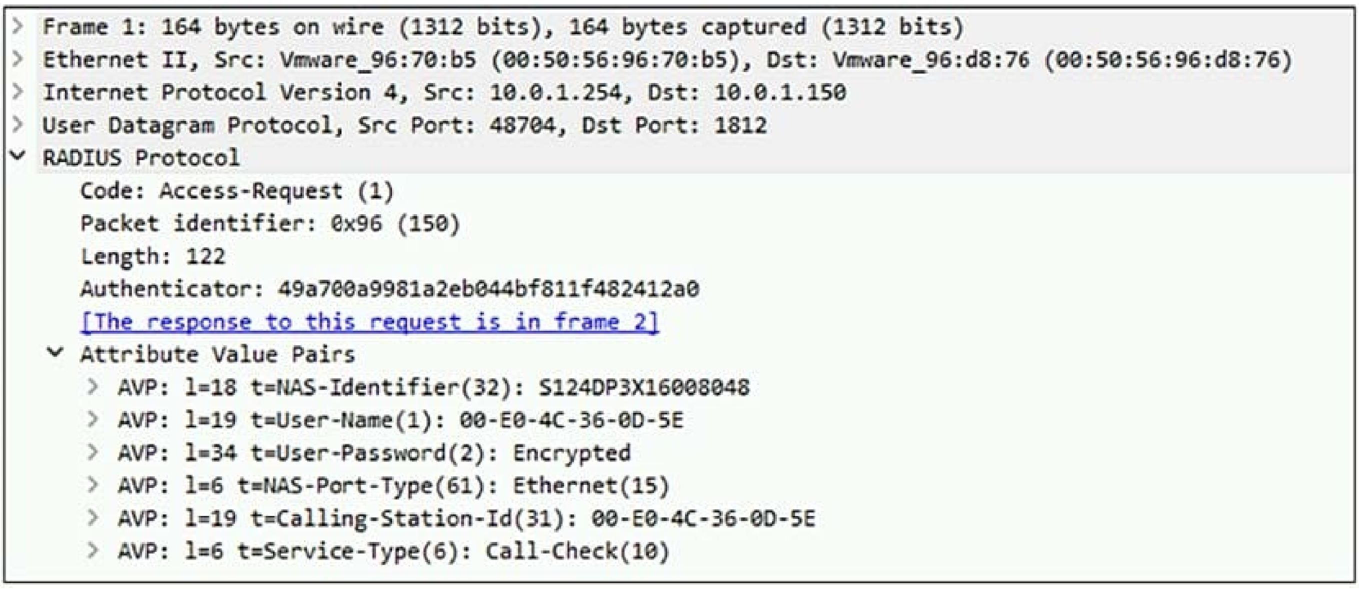
D. Use DHCP option 138 to assign IPs to FortiAP devices.

Correct Answer: C

**QUESTION 2**

Refer to the exhibit.

Examine the packet capture shown in the exhibit, which contains a RADIUS access request packet sent by FortiSwitch to a RADIUS server.



```
> Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
> Ethernet II, Src: Vmware_96:70:b5 (00:50:56:96:70:b5), Dst: Vmware_96:d8:76 (00:50:56:96:d8:76)
> Internet Protocol Version 4, Src: 10.0.1.254, Dst: 10.0.1.150
> User Datagram Protocol, Src Port: 48704, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x96 (150)
    Length: 122
    Authenticator: 49a700a9981a2eb044bf811f482412a0
    [The response to this request is in frame 2]
  v Attribute Value Pairs
    > AVP: l=18 t=NAS-Identifier(32): S124DP3X16008048
    > AVP: l=19 t=User-Name(1): 00-E0-4C-36-0D-5E
    > AVP: l=34 t=User-Password(2): Encrypted
    > AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
    > AVP: l=19 t=Calling-Station-Id(31): 00-E0-4C-36-0D-5E
    > AVP: l=6 t=Service-Type(6): Call-Check(10)
```

Why does the User-Name field in the RADIUS access request packet contain a MAC address?

A. The FortiSwitch interface is configured for 802.1X port authentication with MAC address bypass, and the connected device does not support 802.1X.

B. FortiSwitch authenticates itself using its MAC address as the user name.

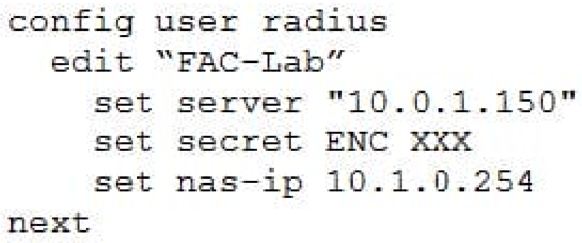
C. The connected device is doing machine authentication.

D. FortiSwitch is replying to an access challenge packet sent by the RADIUS server and requesting the client MAC address.

Correct Answer: D

**QUESTION 3**

Examine the following RADIUS configuration:



```
config user radius
  edit "FAC-Lab"
    set server "10.0.1.150"
    set secret ENC XXX
    set nas-ip 10.1.0.254
next
```

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 notices that the diagnose test authservercommand works with PAP, however, authentication requests fail when using MSCHAPv2.

Which two changes should the administrator make to get MSCHAPv2 to work? (Choose two.)

A. Force FortiGate to use the PAP authentication method in the RADIUS server configuration.

B. Change the remote authentication server from LDAP to RADIUS on FortiAuthenticator.

C. Use MSCHAP instead of using MSCHAPv2

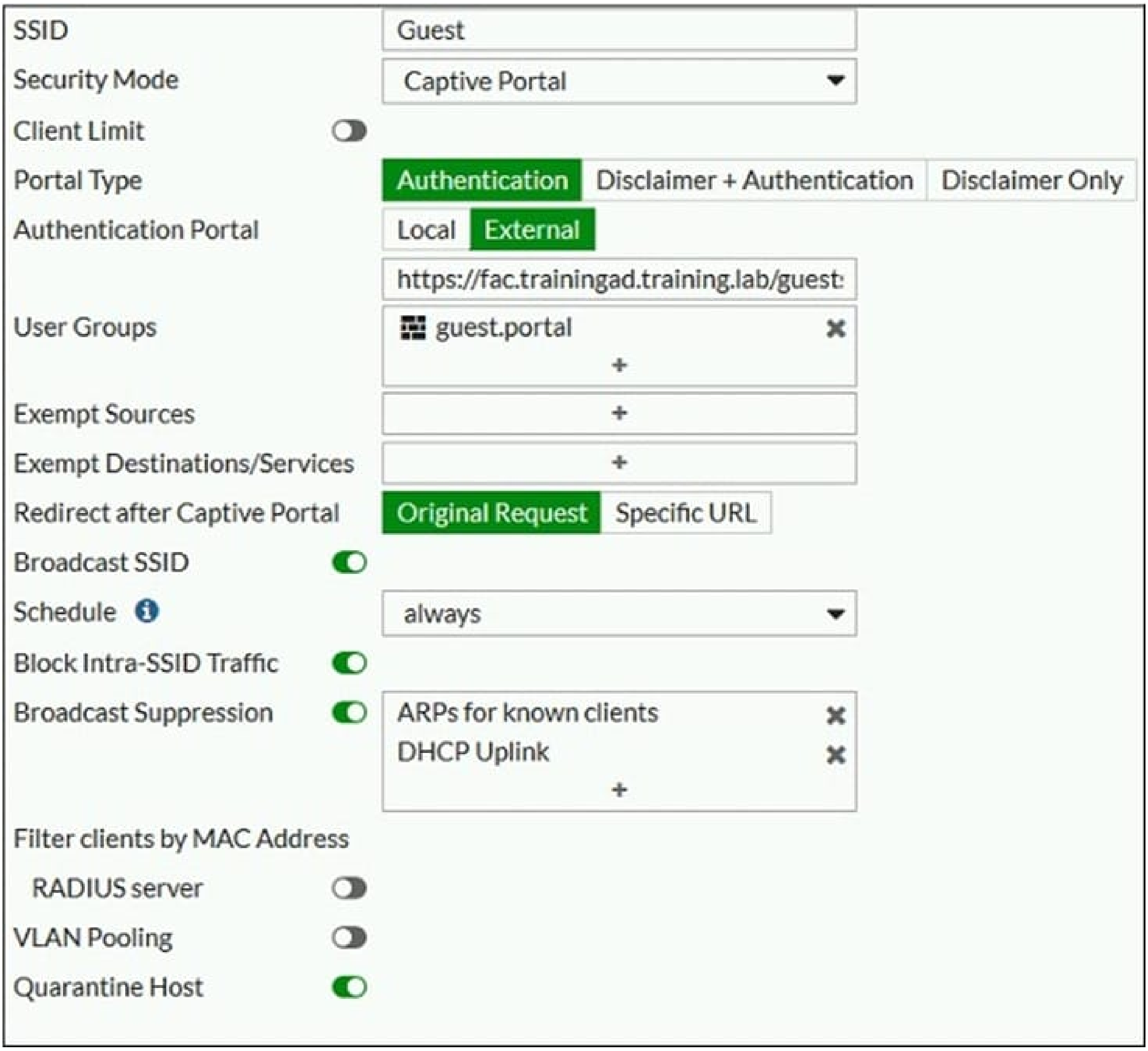
D. Enable Windows Active Directory Domain Authentication on FortiAuthenticator to add FortiAuthenticator to the Windows domain.

Correct Answer: BD

Reference: https://docs.fortinet.com/document/fortiauthenticator/6.0.0/administration-guide/641286/ remote-authentication-servers

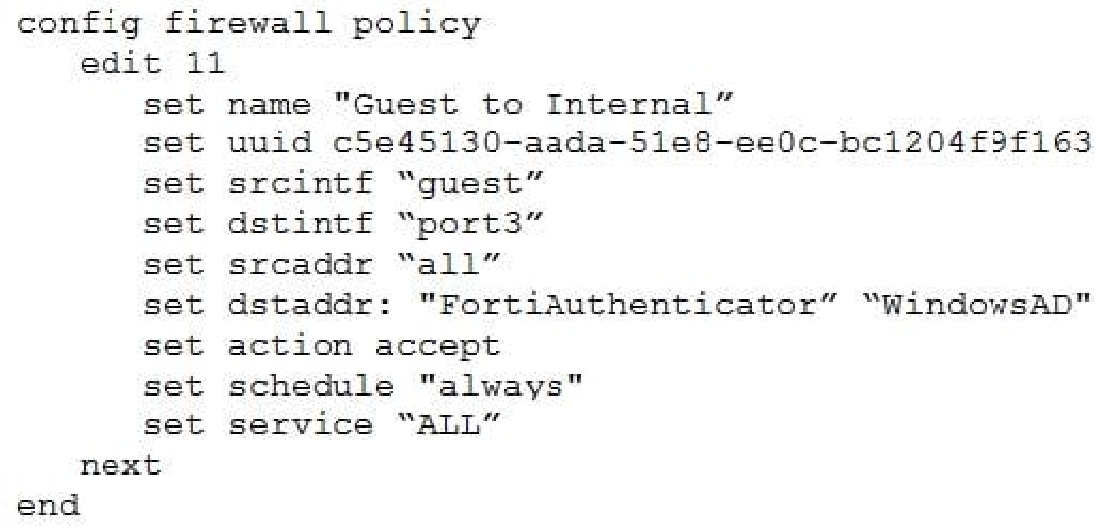
**QUESTION 4**

Refer to the exhibits.



| | | |
|---|---|---|
| SSID | | Guest |
| Security Mode | | Captive Portal ▾ |
| Client Limit | ○ | |
| Portal Type | | [✓ Authentication] Disclaimer + Authentication Disclaimer Only |
| Authentication Portal | | Local [✓ External] |
| | | https://fac.trainingad.training.lab/guest: |
| User Groups | | guest.portal ✖<br>+ |
| Exempt Sources | | + |
| Exempt Destinations/Services | | + |
| Redirect after Captive Portal | | [✓ Original Request] Specific URL |
| Broadcast SSID | ● | |
| Schedule ℹ | | always ▾ |
| Block Intra-SSID Traffic | ● | |
| Broadcast Suppression | ● | ARPs for known clients ✖<br>DHCP Uplink ✖<br>+ |
| Filter clients by MAC Address | | |
| RADIUS server | ○ | |
| VLAN Pooling | ○ | |
| Quarantine Host | ● | |

Examine the firewall policy configuration and SSID settings.



```
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
```

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. Enable the captive-portal-exemptoption in the firewall policy with the ID 11.

B. Apply a guest.portal user group in the firewall policy with the ID 11.

C. Disable the user group from the SSID configuration.

D. Include the wireless client subnet range in the Exempt Source section.

Correct Answer: C

**QUESTION 5**

Which two statements about the use of digital certificates are true? (Choose two.)

A. An intermediate CA can sign server certificates.

B. An intermediate CA can sign another intermediate CA certificate.

C. The end entity\\'s certificate can only be created by an intermediate CA.

D. An intermediate CA can validate the end entity certificate signed by another intermediate CA.

Correct Answer: BD

Latest NSE7_SAC-6.2 Dumps | NSE7_SAC-6.2 VCE Dumps | NSE7_SAC-6.2 Practice Test