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.certbus.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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 2

An administrator is deploying APs that are connecting over an IPsec network. All APs have been configured to connect to FortiGate manually. FortiGate can discover the APs and authorize them. However, FortiGate is unable to establish CAPWAP tunnels to manage the APs.

Which configuration setting can the administrator perform to resolve the problem?

A. Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation.

B. Enable CAPWAP administrative access on the IPsec interface.

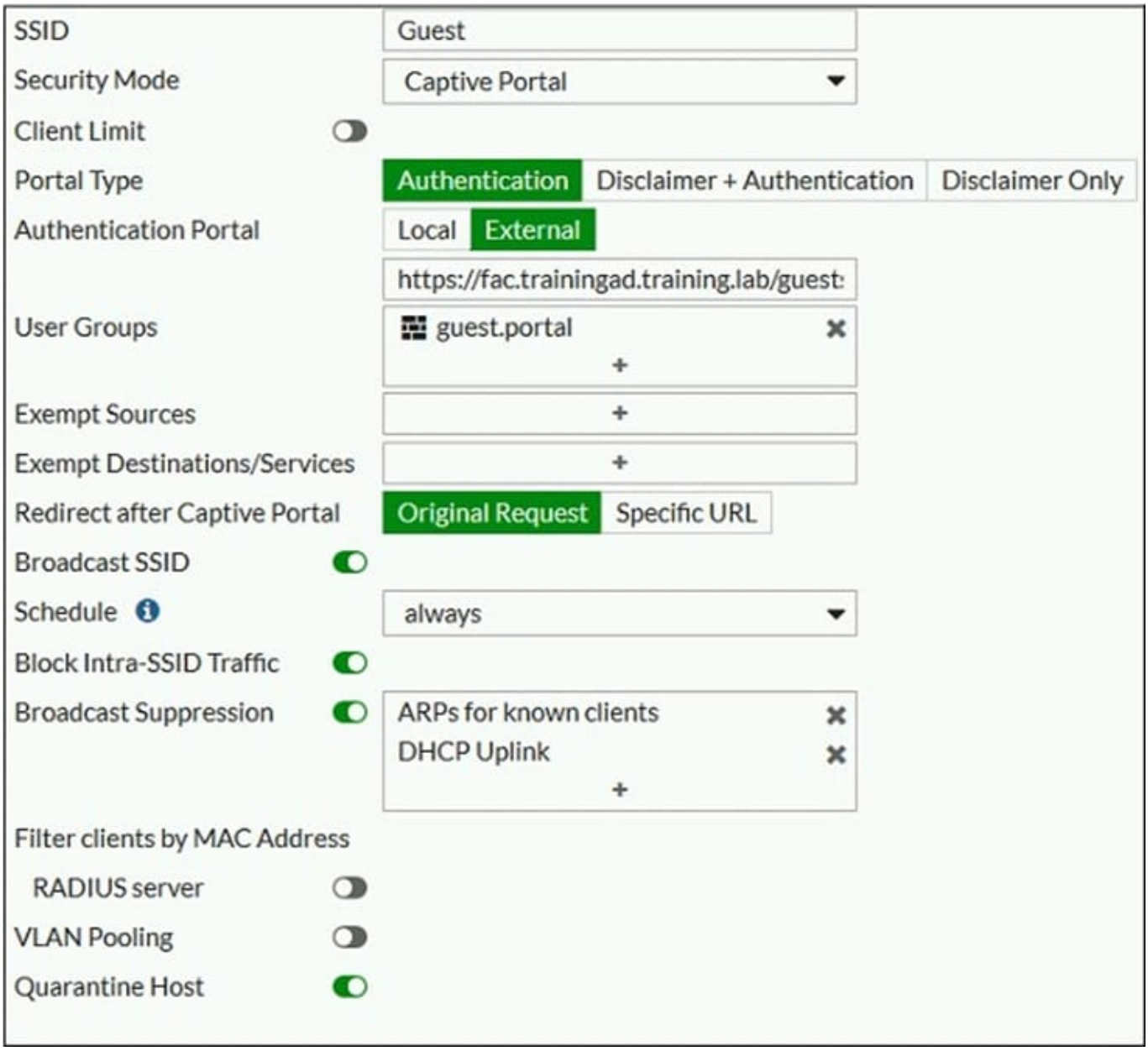
C. Upgrade the FortiAP firmware image to ensure compatibility with the FortiOS version.

D. Assign a custom AP profile for the remote APs with the set mpls-connectionoption enabled.

Correct Answer: B

QUESTION 3

Refer to the exhibits.



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 4

Examine the sections of the configuration shown in the following output:

```
config vpn certificate setting
    set ocsp-status enable
    set ocsp-default-server "FAC"
    set strict-ocsp-check disable
end
config vpn certificate ocsp-server
    edit "FAC"
        set url "http://10.0.1.150:2560"
        set unavail-action revoke
    next
end
config vpn ssl settings
   set ssl-ocsp-option certificate
end
```

What action will the FortiGate take when using OCSP certificate validation?

A. FortiGate will reject the certificate if the OCSP server replies that the certificate is unknown.

B. FortiGate will use the OCSP server 10.0.1.150 even when the OCSP URL field in the user certificate

contains a different OCSP server IP address.

C. FortiGate will use the OCSP server 10.0.1.150 even when there is a different OCSP IP address in the ocsp-override-serveroption under config user peer.

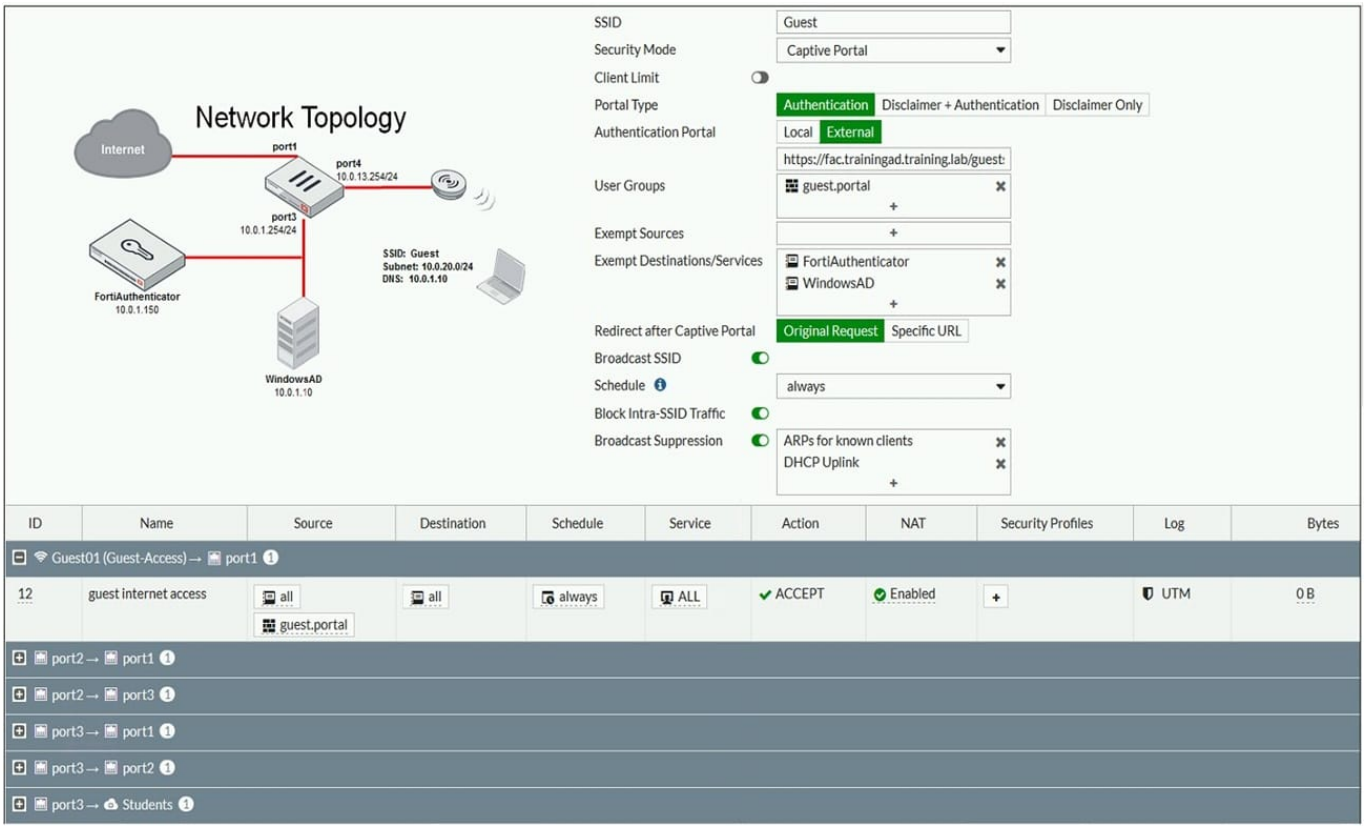
D. FortiGate will invalidate the certificate if the OSCP server is unavailable.

Correct Answer: D

QUESTION 5

Refer to the exhibit.

The exhibit shows 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?

A. Create a firewall policy to allow traffic from the Guest SSID to FortiAuthenticator and Windows AD devices.

B. Enable the captive-portal-exemptoption in the firewall policy with the ID 10.

C. Remove guest.portal user group in the firewall policy.

D. FortiAuthenticator and WindowsAD address objects should be added as exempt sources.

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/868644/captive-portals