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.pass2lead.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

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.

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

An administrator has deployed dual band-capable wireless APs in a wireless network. Multiple 2.4 GHz wireless clients are connecting to the network, and subsequent monitoring shows that individual AP

2.4GHz interfaces are being overloaded with wireless connections. Which configuration change would best resolve the overloading issue?

A. Configure load balancing AP handoff on both the AP interfaces on all APs.

B. Configure load balancing AP handoff on only the 2.4GHz interfaces of all Aps.

C. Configure load balancing frequency handoff on both the AP interfaces.

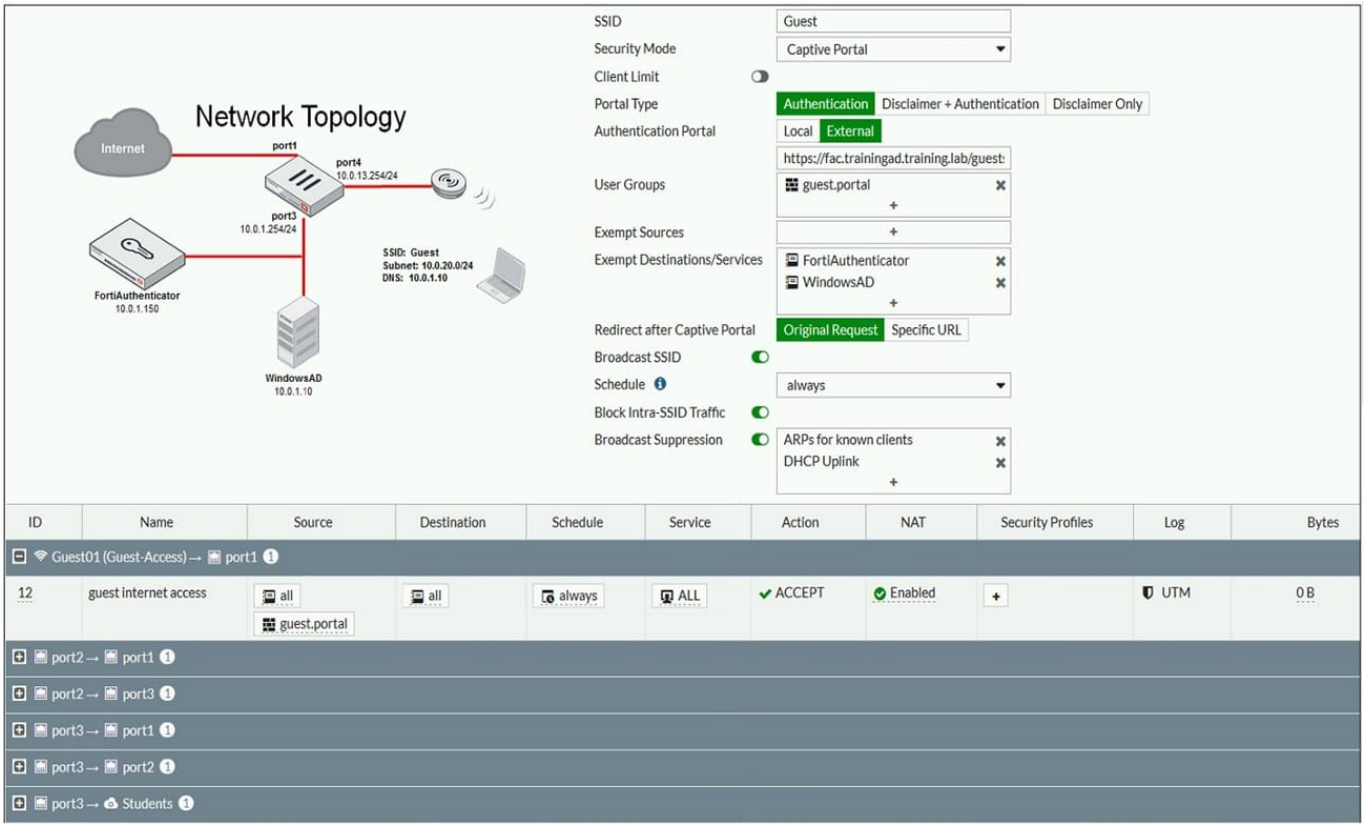
D. Configure a client limit on the all AP 2.4GHz interfaces.

Correct Answer: C

QUESTION 4

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

QUESTION 5

Which two EAP methods can use MSCHAPV2 for client authentication? (Choose two.)

A. PEAP

B. EAP-TTLS

C. EAP-TLS

D. EAP-GTC

Correct Answer: AC

Reference: https://help.fortinet.com/fauth/3-3/Content/FortiAuthenticator%203_3%20Admin%20Guide/500/501_EAP.htm