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.leads4pass.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

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 2

802.1X port authentication is enabled on only those ports that the FortiSwitch security policy is assigned to.

Which configurable items are available when you configure the security policy on FortiSwitch? (Choose two.)

A. FSSO groups

B. Security mode

C. User groups

D. Default guest group

Correct Answer: BC

QUESTION 3

A wireless network in a school provides guest access using a captive portal to allow unregistered users to self-register and access the network. The administrator is requested to update the existing configuration to provide captive portal authentication through a secure connection (HTTPS) to protect and encrypt guest user credentials after they receive the login information when registered for the first time.

Which two changes must the administrator make to enforce HTTPS authentication? (Choose two.)

A. Provide instructions to users to use HTTPS to access the network.

B. Create a new SSID with the HTTPS captive portal URL.

C. Enable Redirect HTTP Challenge to a Secure Channel (HTTPS) in the user authentication settings

D. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator

Correct Answer: BD

QUESTION 4

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 5

What is the purpose of configuring the Windows Active Directory Domain Authentication feature?

A. Allows FortiAuthenticator to register itself as a Windows trusted device to proxy CHAP authentication using Kerberos.

B. Allows FortiAuthenticator to use Windows administrator credentials to perform an LDAP lookup for a user search.

C. Allows FortiAuthenticator to use a Windows CA certificate when authenticating RADIUS users.

D. Allows FortiAuthenticator to authenticate users listed on Windows AD. Enables single sign-on services for VPN and wireless users.

Correct Answer: D

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