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

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

QUESTION 1

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

QUESTION 2

Refer to the exhibit.

```
config wireless-controller wtp-profile
edit "Main Networks - FAP-320C"
        set comment "Profile with standard networks"
        config platform
            set type 320C
        end
        set handoff-rssi 30
        set handoff-sta-thresh 30
        set ap-country GB
        set allowaccess https ssh
        set login-passwd-change yes
        config radio-1
            set band 802.11n,g-only
            set channel-utilization enable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set frequency-handoff enable
            set ap-handoff enable
            set vap-all disable
            set vaps "Guest" "Corporate"
            set channel "1" "6" "11"
        end
        config radio-2
            set band 802.11ac
            set channel-bonding 40MHz
            set channel-utilization enable
            set wids-profile "default-wids-apscan-enabled"
            set darrp enable
            set frequency-handoff enable
            set ap-handoff enable
            set vap-all disable
            set vaps "Guest" "Corporate"
            set channel "36" "44" "52"
        end
    next
end
```

In the WTP profile configuration shown in the exhibit, the AP profile is assigned to two FAP-320 APs that are installed in an open plan office.

1.

The first AP has 32 clients associated to the 5GHz radios and 22 clients associated to the 2.4GHz

radio.

2.

The second AP has 12 clients associated to the 5GHz radios and 20 clients associated to the 2.4GHz radio.

A dual band-capable client enters the office near the first AP and the first AP measures the new client at ?33 dBm signal strength. The second AP measures the new client at ?43 dBm signal strength.

In the new client attempts to connect to the corporate wireless network, to which AP radio will the client be associated?

A. The second AP 5GHz interface.

B. The first AP 2.4GHz interface.

C. The first AP 5GHz interface.

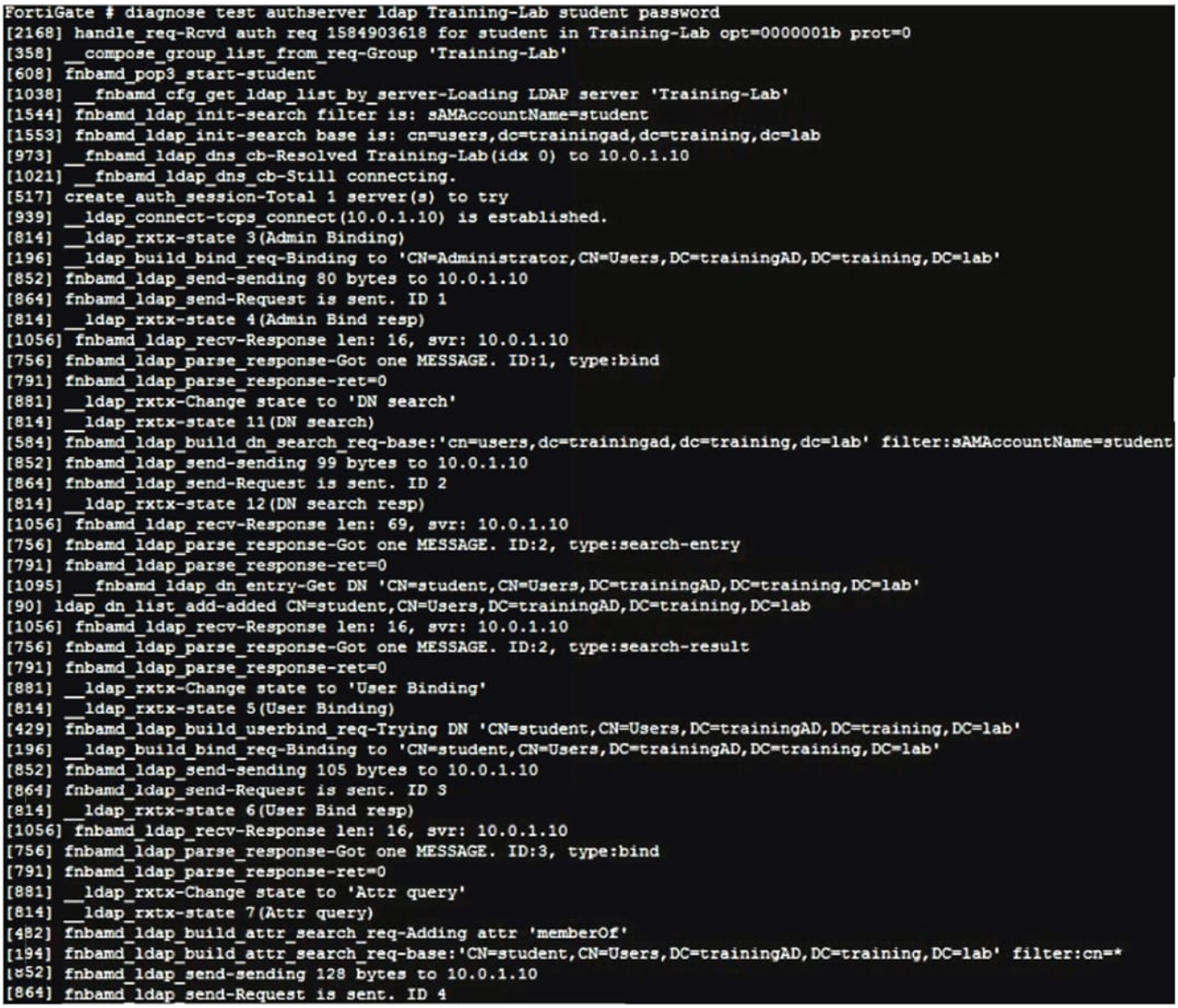
D. The second AP 2.4GHz interface.

Correct Answer: A

QUESTION 3

Refer to the exhibit.

Examine the partial debug output shown in the exhibit.



```
FortiGate # diagnose test authserver ldap Training-Lab student password
[2168] handle_req-Rcvd auth req 1584903618 for student in Training-Lab opt=0000001b prot=0
[358] __compose_group_list_from_req-Group 'Training-Lab'
[608] fnbamd_pop3_start-student
[1038] __fnbamd_cfg_get_ldap_list_by_server-Loading LDAP server 'Training-Lab'
[1544] fnbamd_ldap_init-search filter is: sAMAccountName=student
[1553] fnbamd_ldap_init-search base is: cn=users,dc=trainingad,dc=training,dc=lab
[973] __fnbamd_ldap_dns_cb-Resolved Training-Lab(idx 0) to 10.0.1.10
[1021] __fnbamd_ldap_dns_cb-Still connecting.
[517] create_auth_session-Total 1 server(s) to try
[939] __ldap_connect-tcps_connect(10.0.1.10) is established.
[814] __ldap_rxtx-state 3(Admin Binding)
[196] __ldap_build_bind_req-Binding to 'CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab'
[852] fnbamd_ldap_send-sending 80 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 1
[814] __ldap_rxtx-state 4(Admin Bind resp)
[1056] fnbamd_ldap_recv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:1, type:bind
[791] fnbamd_ldap_parse_response-ret=0
[881] __ldap_rxtx-Change state to 'DN search'
[814] __ldap_rxtx-state 11(DN search)
[584] fnbamd_ldap_build_dn_search_req-base:'cn=users,dc=trainingad,dc=training,dc=lab' filter:sAMAccountName=student
[852] fnbamd_ldap_send-sending 99 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 2
[814] __ldap_rxtx-state 12(DN search resp)
[1056] fnbamd_ldap_recv-Response len: 69, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-entry
[791] fnbamd_ldap_parse_response-ret=0
[1095] __fnbamd_ldap_dn_entry-Get DN 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[90] ldap_dn_list_add-added CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab
[1056] fnbamd_ldap_recv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-result
[791] fnbamd_ldap_parse_response-ret=0
[881] __ldap_rxtx-Change state to 'User Binding'
[814] __ldap_rxtx-state 5(User Binding)
[429] fnbamd_ldap_build_userbind_req-Trying DN 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[196] __ldap_build_bind_req-Binding to 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[852] fnbamd_ldap_send-sending 105 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 3
[814] __ldap_rxtx-state 6(User Bind resp)
[1056] fnbamd_ldap_recv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:3, type:bind
[791] fnbamd_ldap_parse_response-ret=0
[881] __ldap_rxtx-Change state to 'Attr query'
[814] __ldap_rxtx-state 7(Attr query)
[482] fnbamd_ldap_build_attr_search_req-Adding attr 'memberOf'
[194] fnbamd_ldap_build_attr_search_req-base:'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab' filter:cn=*
[852] fnbamd_ldap_send-sending 128 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 4
```

Which two statements about the debug output are true? (Choose two.)

A. The connection to the LDAP server timed out.

B. The user authenticated successfully.

C. The LDAP server is configured to use regular bind.

D. The debug output shows multiple user authentications.

Correct Answer: BC

QUESTION 4

A FortiGate has the following LDAP configuration.

```
config user ldap
   edit "Training-Lab"
      set server "10.0.1.10"
      set cnid "cn"
      set dn "cn=users,dc=trainingad,dc=training,dc=lab"
      set type regular
      set username "CN=Administrator,DC=trainingAD,DC=training,DC=lab"
      set password ENC XXX
next
```

On the Windows LDAP server 10.0.1.10, the administrator used dsquery, which returned the following output:

>dsquery user -samid admin*

"CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab"

According to the output, which FortiGate LDAP setting is configured incorrectly?

A. dn

B. sAMAccountName

C. username

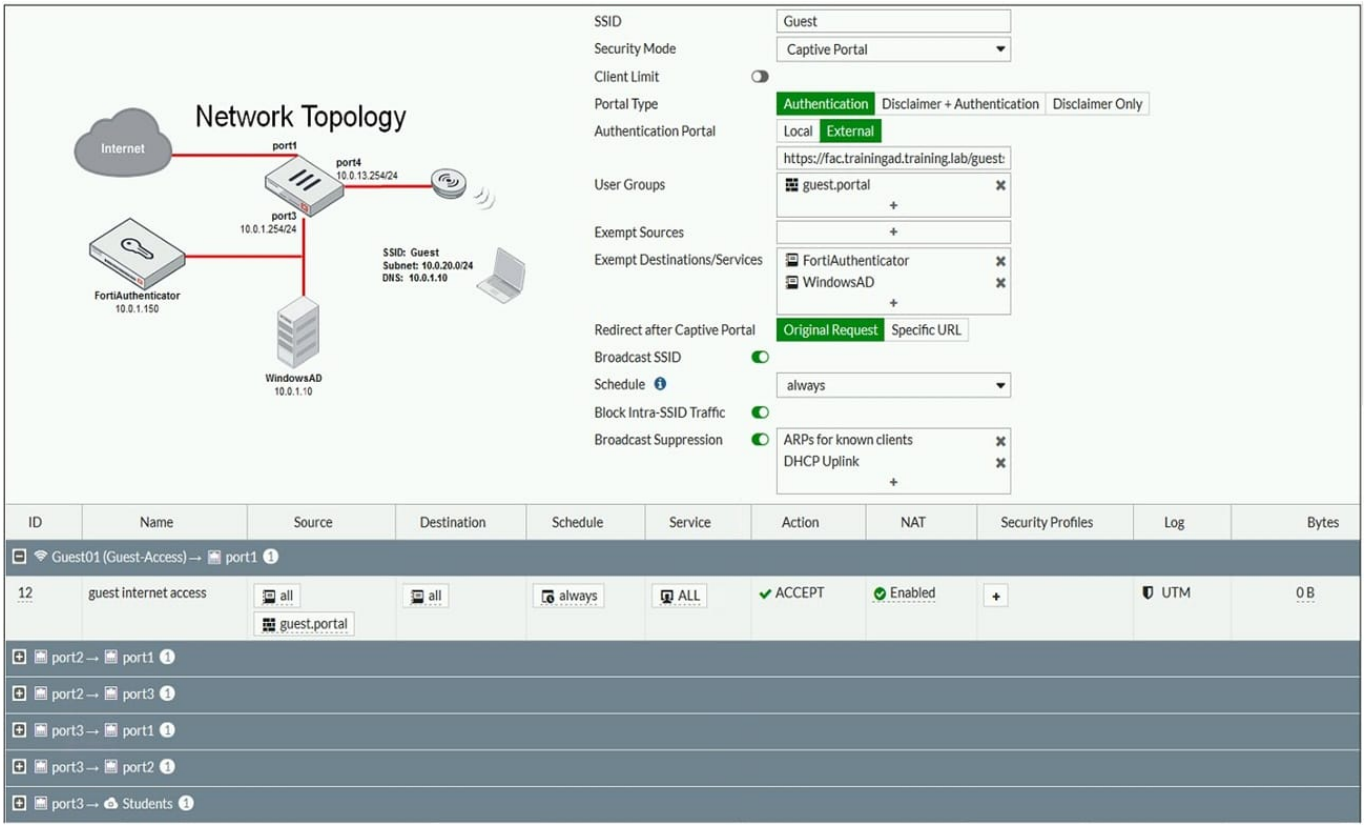
D. cnid

Correct Answer: B

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