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.pass4itsure.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

Refer to the exhibits.

```
config wireless-controller vap
    edit "Corp"
        set vdom "root"
        set ssid "Corp"
        set security wpa2-only-enterprise
        set auth radius
        set radius-server "FAC-Lab"
        set intra-vap-privacy enabled
        set schedule "always"
        set vlan-pooling wtp-group
        config vlan-pool
            edit 101
                set wtp-group "Floor 1"
            next
            edit 102
                set wtp-group "Office"
            next
        end
    next
```

Examine the VAP configuration and the WiFi zones table shown in the exhibits.

WiFi (1)						
	Corp ((•)) SSID: Corp)	10.0.3.1 255.255.255.0		🛜 WiFi SSID	3	
Zone (3)						
⊟	Corp.zone			☐ Zone	0	
⋮⋯	Corp.101	0.0.0.0 0.0.0.0		🔒 VLAN	1	101
⋮⋯	Corp.102	10.0.20.1 255.255.255.0		🔒 VLAN	2	102

Which two statements describe FortiGate behavior regarding assignment of VLANs to wireless clients? (Choose two.)

A. FortiGate will load balance clients using VLAN 101 and VLAN 102 and assign them an IP address from the 10.0.3.0/24 subnet.

B. Clients connecting to APs in the Floor 1 group will not be able to receive an IP address.

C. All clients connecting to the Corp SSID will receive an IP address from the 10.0.3.1/24 subnet.

D. Clients connecting to APs in the Office group will be assigned an IP address from the 10.0.20.1/24 subnet.

Correct Answer: BD

QUESTION 2

Refer to the exhibit.

```
FortiGate # diagnose switch-controller switch-info 802.1X
Managed Switch : S224EPTF18001736

    port2 : Mode: port-based (mac-by-pass disable)
            Link: Link up
            Port State: unauthorized: (  )
            Dynamic Authorized Vlan : 0
            EAP pass-through mode : Enable
            Quarantine VLAN (4093) detection : Enable
            Native Vlan : 10
            Allowed Vlan list: 10,4093
            Untagged Vlan list: 4093
            Guest VLAN :
            Auth-Fail Vlan :

            Sessions info:
            00:09:0f:02:02:02      Type=802.1x,,state=AUTHENTICATING,etime=0,eap_cnt=0 params:reAuth=3600
```

A host machine connected to port2 on FortiSwitch cannot connect to the network. All ports on FortiSwitch are assigned a security policy to enforce 802.1X port authentication. While troubleshooting the issue, the administrator runs the debug command and obtains the output shown in the exhibit.

Which two scenarios are the likely cause of this issue? (Choose two.)

A. The host machine is not configured for 802.1X port authentication.

B. The host machine does not support 802. 1X authentication.

C. The host machine is quarantined due to a security incident.

D. The host machine is configured with wrong VLAN ID.

Correct Answer: AB

Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD46428

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

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 5

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