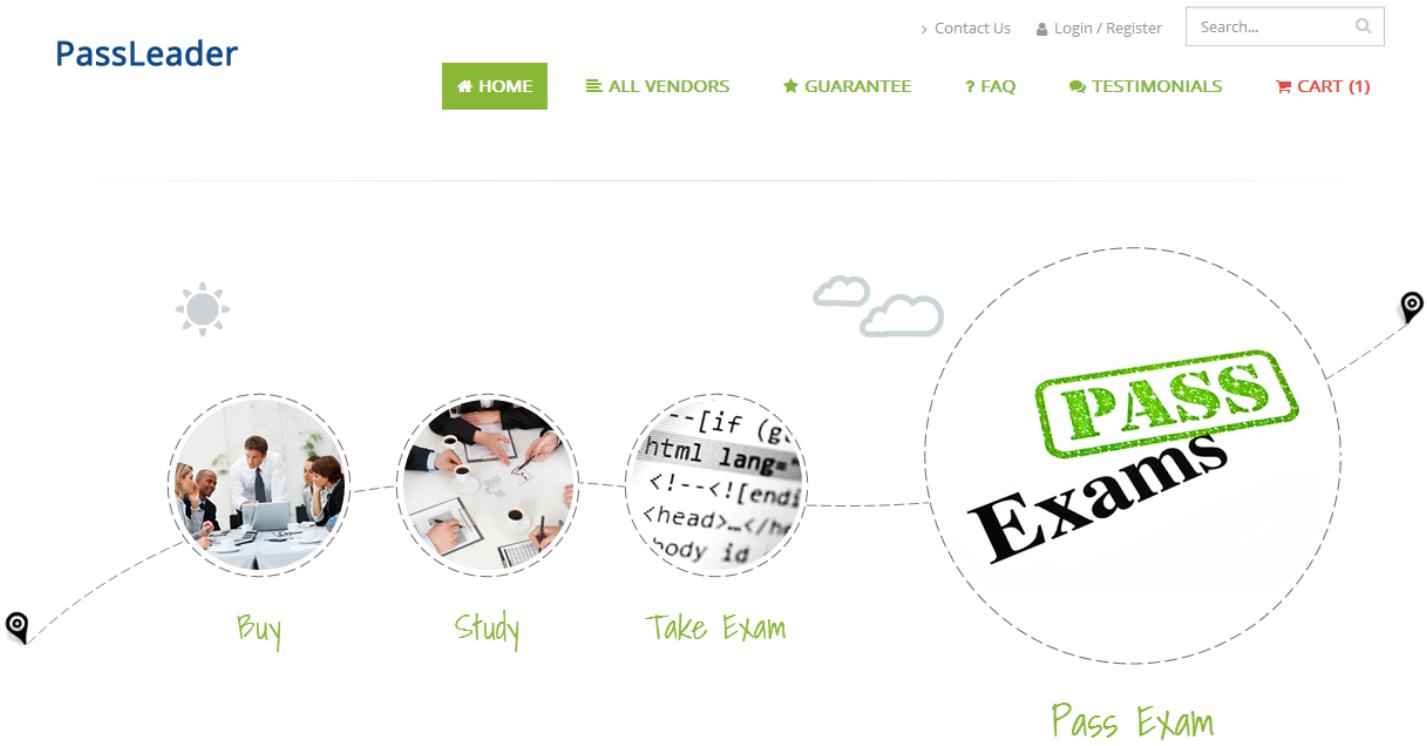
PassLeader



Try **PDF Demo** before you buy

We're not the only ones **happy** about PassLeader Practice Material ...

63159+ customers in 100+ countries use PassLeader Test Engine. Meet our customers.

VOREED GetCustom JET ORANGE iCompany Paradoxx iMessenger

http://www.passleader.top/

Latest Exam Guide & Learning Materials

Exam : **NSE7_LED-7.0**

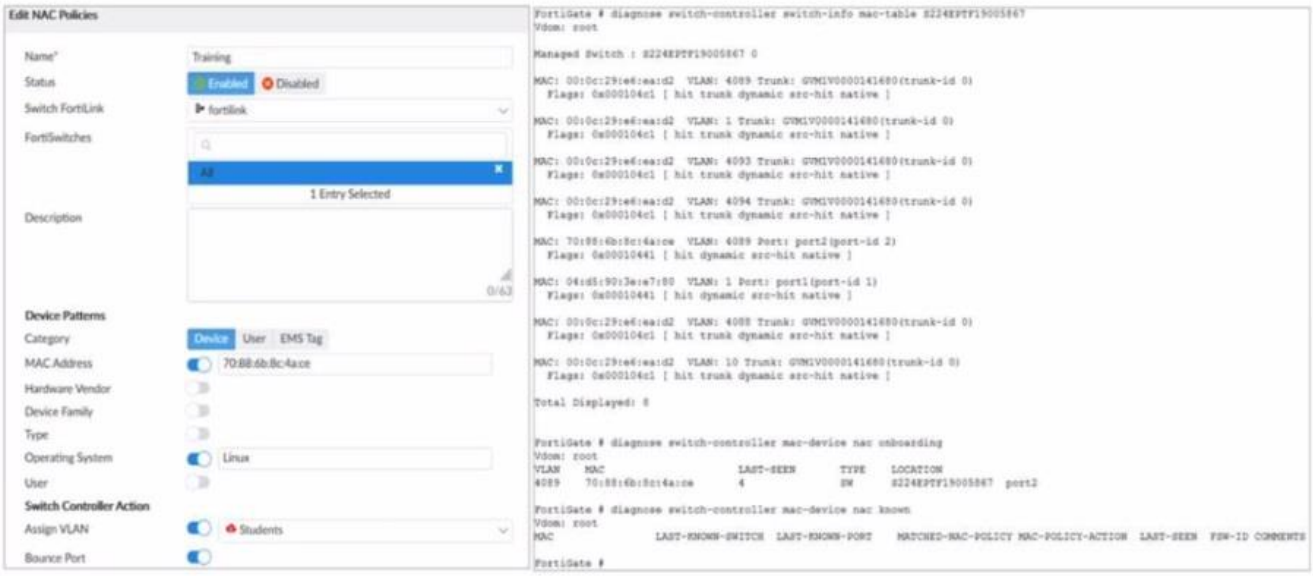
Title : Fortinet NSE 7 - LAN Edge 7.0

Vendor : Fortinet

Version : DEMO

QUESTION NO: 1
Which two pieces of information can the diagnose test authserver ldap command provide? (Choose two.)
A. It displays whether the admin bind user credentials are correct
B. It displays whether the user credentials are correct
C. It displays the LDAP codes returned by the LDAP server
D. It displays the LDAP groups found for the user
Answer: B D

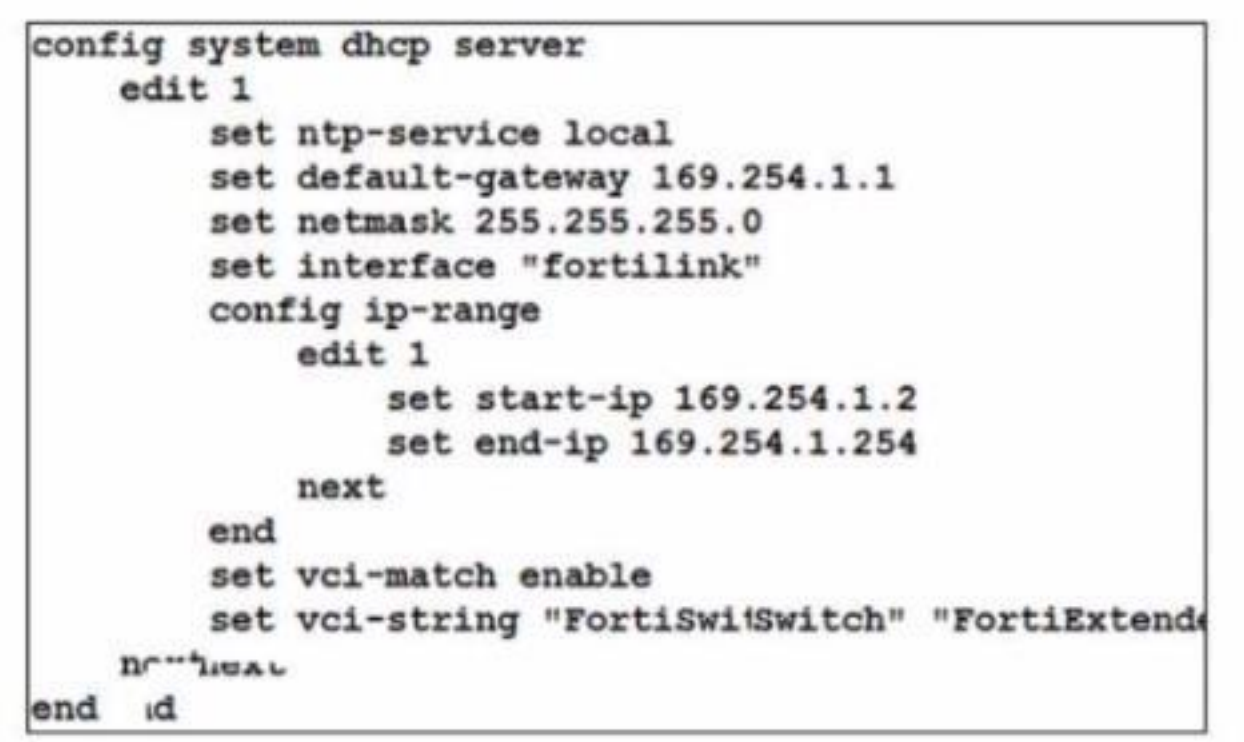
QUESTION NO: 2
Refer to the exhibit.



Examine the FortiManager configuration and FortiGate CLI output shown in the exhibit An administrator is testing the NAC feature The test device is connected to a managed FortiSwitch device
{S224EPTF19"53€7)onport2
After applying the NAC policy on port2 and generating traffic on the test device the test device is not matching the NAC policy therefore the test device remains m the onboarding VLAN Based on the information shown in the exhibit which two scenarios are likely to cause this issue? (Choose two.)
A. Management communication between FortiGate and FortiSwitch is down
B. The MAC address configured on the NAC policy is incorrect
C. The device operating system detected by FortiGate is not Linux
D. Device detection is not enabled on VLAN 4089
Answer: C D
Explanation:
According to the FortiManager configuration, the NAC policy is set to match devices with the MAC address of 00:0c:29:6a:2b:3c and the operating system of Linux. However, according to the FortiGate CLI output, the test device has a different MAC address of 00:0c:29:6a:2b:3d. Therefore, option B is true. Option A is also true because the FortiSwitch device status is shown as down, which means that the management communication betweenFortiGate and

FortiSwitch is not working properly. This could prevent the NAC policy from being applied correctly. Option C is false because the device operating system detected by FortiGate is Linux, which matches the NAC policy. Option D is false because device detection is enabled on VLAN 4089, as shown by the command "config switch-controller vlan".

QUESTION NO: 3
Refer to the exhibit.



By default FortiOS creates the following DHCP server scope for the FortiLink interface as shown in the exhibit What is the objective of the vci-string setting?

A. To ignore DHCP requests coming from FortiSwitch and FortiExtender devices

B. To reserve IP addresses for FortiSwitch and FortiExtender devices

C. To restrict the IP address assignment to FortiSwitch and FortiExtender devices

D. To restrict the IP address assignment to devices that have FortiSwitch or FortiExtender as their hostname

Answer: C

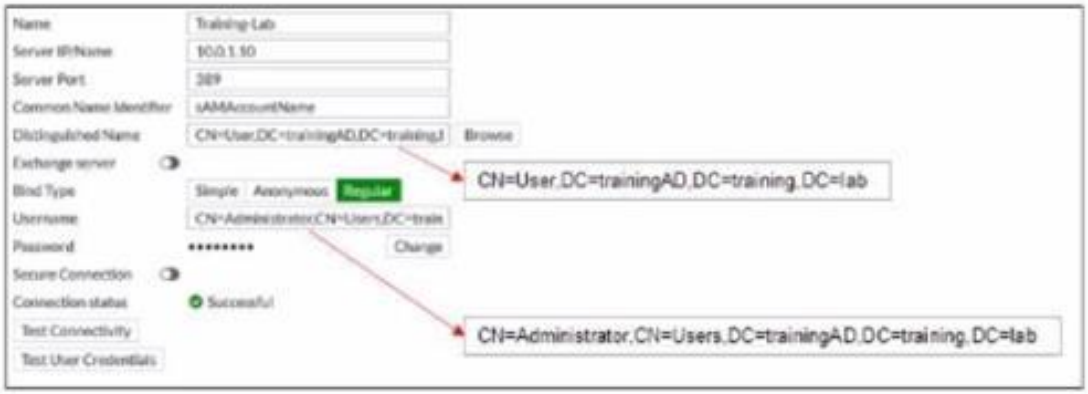
Explanation:

According to the exhibit, the DHCP server scope for the FortiLink interface has a vci-string setting with the value "Cisco AP c2700". This setting is used to match the vendor class identifier (VCI) of the DHCP clients that request an IP address from the DHCP server. The VCI is a text string that uniquely identifies a type of vendor device. Therefore, option C is true because the vci-string setting restricts the IP address assignment to FortiSwitch and FortiExtender devices, which use the VCI "Cisco AP c2700". Option A is false because the vci-string setting does not ignore DHCP requests coming from FortiSwitch and FortiExtender devices, but rather accepts them. Option B is false because the vci-string setting does not reserve IP addresses for FortiSwitch and FortiExtender devices, but rather assigns them dynamically. Option D is false because the vci- string setting does not restrict the IP address

assignment to devices that have FortiSwitch or FortiExtender as their hostname, but rather to devices that have "Cisco AP c2700" as their VCI.

QUESTION NO: 4
Which EAP method requires the use of a digital certificate on both the server end and the client end?
A. EAP-TTLS
B. PEAP
C. EAP-GTC
D. EAP-TLS
Answer: D
Explanation:
According to the FortiGate Administration Guide, "EAP-TLS is the most secure EAP method. It requires a digital certificate on both the server end and the client end. The server and client authenticate each other using their certificates." Therefore, option D is true because it describes the EAP method that requires the use of a digital certificate on both the server end and the client end. Option A is false because EAP-TTLS only requires a digital certificate on the server end, not the client end. Option B is false because PEAP also only requires a digital certificate on the server end, not the client end. Option C is false because EAP-GTC does not require a digital certificate on either the server end or the client end.

QUESTION NO: 5
Refer to the exhibits.
Exhibit



Examine the LDAP server configuration and output shown in the exhibits.

Exhibit

```
FortiGate # diagnose test authserver ldap Training-Lab student password
[1909] handle_req-Rcvd auth req 1035874260 for student in Training-Lab opt=0000001b prot=0
[466] __compose_group_list_from_req-Group 'Training-Lab', type 1
[617] fnbamd_pop3_start-student
[976] __fnbamd_cfg_get_ldap_list_by_server-
[2238] fnbamd_user_ldap_create-LDAP servers are created, vfid=0, total=1
[982] __fnbamd_cfg_get_ldap_list_by_server-Loaded LDAP server 'Training-Lab'
[1137] fnbamd_cfg_get_ldap_list-Total ldap servers to try: 1
[1718] fnbamd_ldap_init-search filter is: sAMAccountName=student
[1727] fnbamd_ldap_init-search base is: cn=user,dc=trainingad,dc=training,dc=lab
[1151] __fnbamd_ldap_dns_cb-Resolved Training-Lab:10.0.1.10 to 10.0.1.10, cur stack size:1
[924] __fnbamd_ldap_get_next_addr-
[1157] __fnbamd_ldap_dns_cb-Connection starts Training-Lab:10.0.1.10, addr 10.0.1.10
[879] __fnbamd_ldap_start_conn-Still connecting 10.0.1.10.
[633] create_auth_session-Total 1 server(s) to try
[1108] __ldap_connect-tcps_connect(10.0.1.10) is established.
[986] __ldap_rxtx-state 3(Admin Binding)
[363] __ldap_build_bind_req-Binding to 'CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=l
[1084] fnbamd_ldap_send-sending 80 bytes to 10.0.1.10
[1096] fnbamd_ldap_send-Request is sent. ID 1
[986] __ldap_rxtx-state 4(Admin Bind resp)
[1127] __fnbamd_ldap_read-Read 8
[1233] fnbamd_ldap_recv-Leftover 2
[1127] __fnbamd_ldap_read-Read 14
```

Exhibit

```
:307] fnbamd_bamd_ldap_recv-Response len: 16, svr: 10.0.1.10
:89] fnbamd_lamd_ldap_parse_response-Got one MESSAGE. ID:1, type:bind
:023] fnbamd_bamd_ldap_parse_response-ret=0
:053] __ldap_ldap_rxtx-Change state to 'DN search'
:86] __ldap_ldap_rxtx-state 11(DN search)
:51] fnbamd_lamd_ldap_build_dn_search_req-base:'cn=user,dc=trainingad,dc=training,dc=lab' filter:sAMAccountName=student
:054] fnbamd_bamd_ldap_send-sending 98 bytes to 10.0.1.10
:096] fnbamd_bamd_ldap_send-Request is sent. ID 2
:86] __ldap_ldap_rxtx-state 12(DN search resp)
:127] __fnbamfnbamd_ldap_read-Read 8
:233] fnbamd_bamd_ldap_recv-Leftover 2
:127] __fnbamfnbamd_ldap_read-Read 166
:307] fnbamd_bamd_ldap_recv-Response len: 168, svr: 10.0.1.10
:89] fnbamd_lamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-result
:010] fnbamd_bamd_ldap_parse_response-Error 32(0000208D: NameErr: DSID-03100213, problem 2001 (NO_OBJECT), data 0, best match
      'DC=tDC=trainingAD,DC=training,DC=lab'

:023] fnbamd_bamd_ldap_parse_response-ret=32
:85] __ldap_ldap_done-svr 'Training-Lab'
:55] __ldap_ldap_destroy-
:25] __ldap_ldap_stop-Conn with 10.0.1.10 destroyed.
:17] fnbamd_cmd_comm_send_result-Sending result 1 (nid 0) for req 1035874260, len=2149
thenticate 'st= 'student' against 'Training-Lab' failed!
```

Note that the Distinguished Name and Username settings on the LDAP server configuration have been expanded to display their full contents.
An LDAP user named student cannot authenticate. While testing the student account, the administrator gets the CLI output shown in the exhibit.
According to the output, which FortiGate LDAP server settings must the administrator check?

A. Distinguished Name

B. Bind Type

C. Common Name Identifier

D. Username

Answer: D

QUESTION NO: 6

What is the purpose of enabling Windows Active Directory Domain Authentication on FortiAuthenticator?

A. It enables FortiAuthenticator to use Windows administrator credentials to perform an

LDAP lookup for a user search

B. It enables FortiAuthenticator to use a Windows CA certificate when authenticating RADIUS users

C. It enables FortiAuthenticator to import users from Windows AD

D. It enables FortiAuthenticator to register itself as a Windows trusted device to proxy authentication using Kerberos

Answer: D

Explanation:

According to the FortiAuthenticator Administration Guide2, "Windows Active Directory domain authentication enables FortiAuthenticator to join a Windows Active Directory domain as a machine entity and proxy authentication requests using Kerberos." Therefore, option D is true because it describes the purpose of enabling Windows Active Directory domain authentication on FortiAuthenticator. Option A is false because FortiAuthenticator does not need Windows administrator credentials to perform an LDAP lookup for a user search. Option B is false because FortiAuthenticator does not use a Windows CA certificate when authenticating RADIUS users, but rather its own CA certificate. Option C is false because FortiAuthenticator does not import users from Windows AD, but rather synchronizes them using LDAP or FSSO.