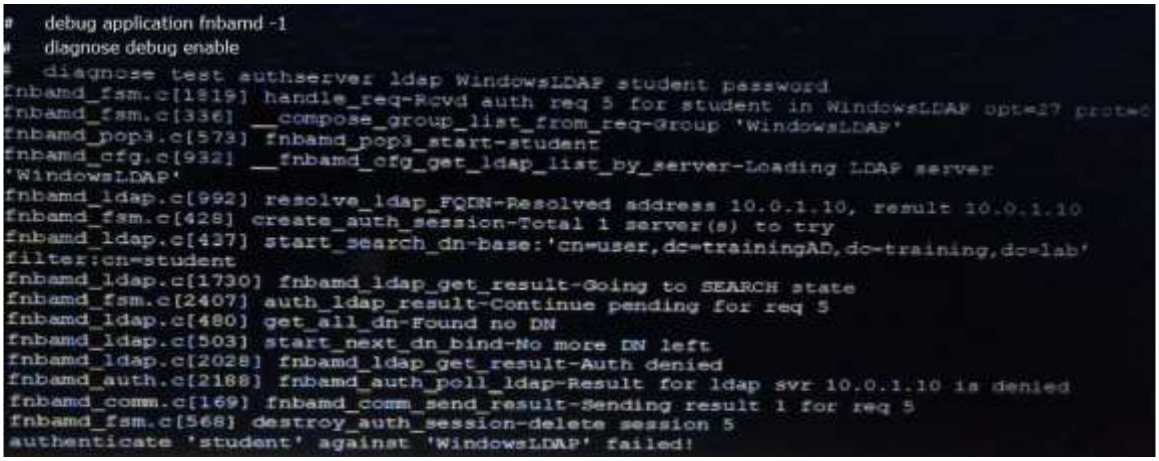
Vendor: Fortinet

Exam Code: NSE7_EFW

Exam Name: Enterprise Firewall - FortiOS 5.4

Version: DEMO

QUESTION 1
An LDAP user cannot authenticate against a FortiGate device. Examine the real time debug output shown in the exhibit when the user attempted the authentication; then answer the question below.



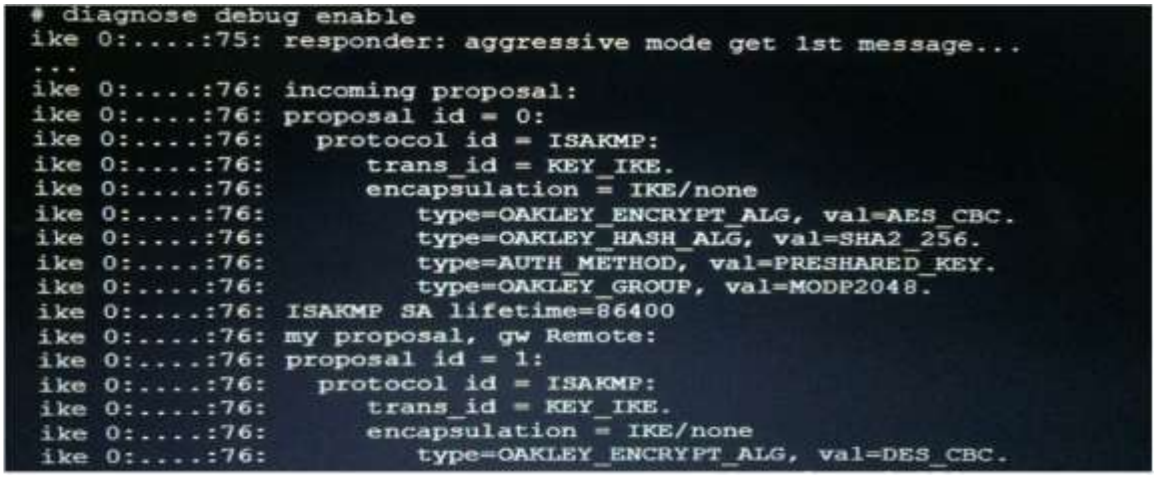
```
#    debug application fnbamd -1
#    diagnose debug enable
#    diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd auth req 5 for student in WindowsLDAP opt=27 prot=0
fnbamd_fsm.c[336] __compose_group_list_from_req-Group 'WindowsLDAP'
fnbamd_pop3.c[573] fnbamd_pop3_start-student
fnbamd_cfg.c[932] __fnbamd_cfg_get_ldap_list_by_server-Loading LDAP server
'WindowsLDAP'
fnbamd_ldap.c[992] resolve_ldap_FQDN-Resolved address 10.0.1.10, result 10.0.1.10
fnbamd_fsm.c[428] create_auth_session-Total 1 server(s) to try
fnbamd_ldap.c[437] start_search_dn-base:'cn=user,dc=trainingAD,dc=training,dc=lab'
filter:cn=student
fnbamd_ldap.c[1730] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[2407] auth_ldap_result-Continue pending for req 5
fnbamd_ldap.c[480] get_all_dn-Found no DN
fnbamd_ldap.c[503] start_next_dn_bind-No more DN left
fnbamd_ldap.c[2028] fnbamd_ldap_get_result-Auth denied
fnbamd_auth.c[2188] fnbamd_auth_poll_ldap-Result for ldap svr 10.0.1.10 is denied
fnbamd_comm.c[169] fnbamd_comm_send_result-Sending result 1 for req 5
fnbamd_fsm.c[568] destroy_auth_session-delete session 5
authenticate 'student' against 'WindowsLDAP' failed!
```

Based on the output in the exhibit, what can cause this authentication problem?

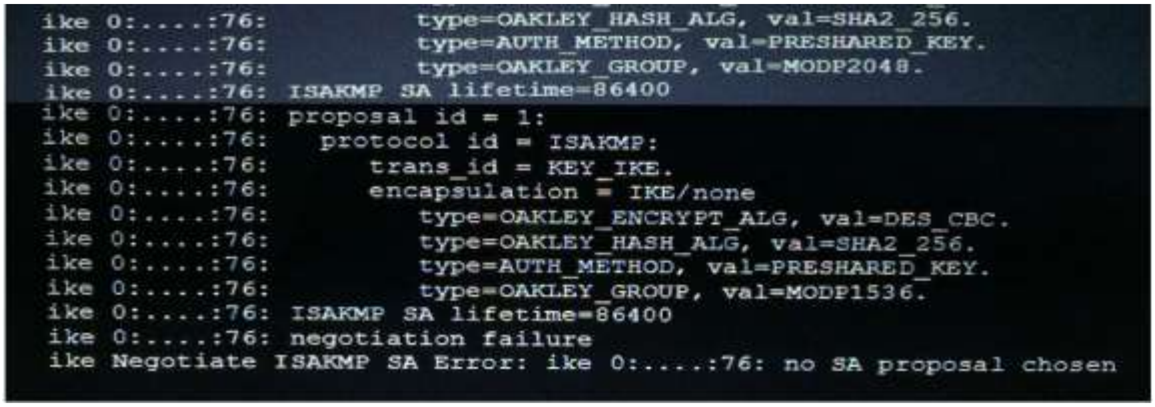
A. User student is not found in the LDAP server.
B. User student is using a wrong password.
C. The FortiGate has been configured with the wrong password for the LDAP administrator.
D. The FortiGate has been configured with the wrong authentication schema.

Answer: A

QUESTION 2
Examine the partial output from the IKE realtime debug shown in the exhibit; then answer the question below.



```
# diagnose debug enable
ike 0:....:75: responder: aggressive mode get 1st message...
...
ike 0:....:76: incoming proposal:
ike 0:....:76: proposal id = 0:
ike 0:....:76:   protocol id = ISAKMP:
ike 0:....:76:      trans_id = KEY_IKE.
ike 0:....:76:      encapsulation = IKE/none
ike 0:....:76:         type=OAKLEY_ENCRYPT_ALG, val=AES_CBC.
ike 0:....:76:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:....:76:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:....:76:         type=OAKLEY_GROUP, val=MODP2048.
ike 0:....:76: ISAKMP SA lifetime=86400
ike 0:....:76: my proposal, gw Remote:
ike 0:....:76: proposal id = 1:
ike 0:....:76:   protocol id = ISAKMP:
ike 0:....:76:      trans_id = KEY_IKE.
ike 0:....:76:      encapsulation = IKE/none
ike 0:....:76:         type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
```



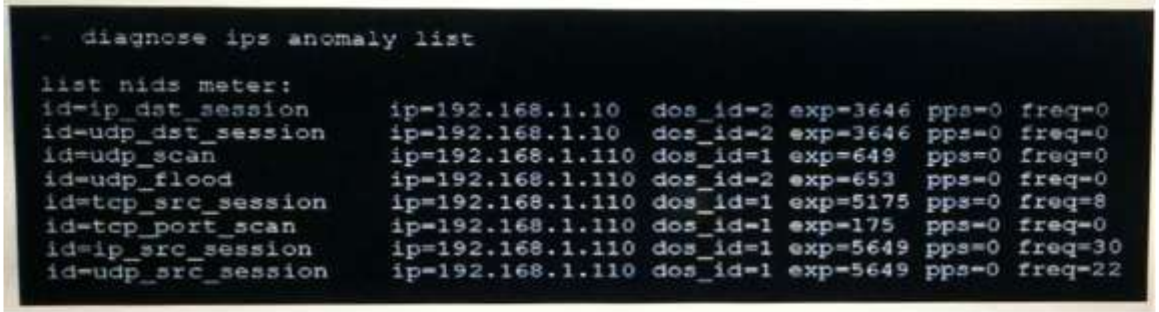
```
ike 0:....:76:              type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:....:76:              type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:....:76:              type=OAKLEY_GROUP, val=MODP2048.
ike 0:....:76: ISAKMP SA lifetime=86400
ike 0:....:76: proposal id = 1:
ike 0:....:76:   protocol id = ISAKMP:
ike 0:....:76:      trans_id = KEY_IKE.
ike 0:....:76:      encapsulation = IKE/none
ike 0:....:76:         type=OAKLEY_ENCRYPT_ALG, val=DES_CBC.
ike 0:....:76:         type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:....:76:         type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:....:76:         type=OAKLEY_GROUP, val=MODP1536.
ike 0:....:76: ISAKMP SA lifetime=86400
ike 0:....:76: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:....:76: no SA proposal chosen
```

Why didn't the tunnel come up?

A. IKE mode configuration is not enabled in the remote IPsec gateway.
B. The remote gateway's Phase-2 configuration does not match the local gateway's phase-2 configuration.
C. The remote gateway's Phase-1 configuration does not match the local gateway's phase-1 configuration.
D. One IPsec gateway is using main mode, while the other IPsec gateway is using aggressive mode.

Answer: B

QUESTION 3
Examine the output of the 'diagnose ips anomaly list' command shown in the exhibit; then answer the question below.



```
-  diagnose ips anomaly list

list nids meter:
id=ip_dst_session       ip=192.168.1.10  dos_id=2 exp=3646 pps=0 freq=0
id=udp_dst_session      ip=192.168.1.10  dos_id=2 exp=3646 pps=0 freq=0
id=udp_scan             ip=192.168.1.110 dos_id=1 exp=649  pps=0 freq=0
id=udp_flood            ip=192.168.1.110 dos_id=2 exp=653  pps=0 freq=0
id=tcp_src_session      ip=192.168.1.110 dos_id=1 exp=5175 pps=0 freq=8
id=tcp_port_scan        ip=192.168.1.110 dos_id=1 exp=175  pps=0 freq=0
id=ip_src_session       ip=192.168.1.110 dos_id=1 exp=5649 pps=0 freq=30
id=udp_src_session      ip=192.168.1.110 dos_id=1 exp=5649 pps=0 freq=22
```

Which IP addresses are included in the output of this command?

A. Those whose traffic matches a DoS policy.
B. Those whose traffic matches an IPS sensor
C. Those whose traffic exceeded a threshold of a matching DoS policy.
D. Those whose traffic was detected as an anomaly by an IPS sensor.

Answer: A

QUESTION 4
Examine the following partial outputs from two routing debug commands; then answer the question below.

```
# get router info routing-table database
s 0.0.0.0/0 [20/0] via 10.200.2.254, port2, [10/0]
s *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1
# get router info routing-table all
s* 0.0.0.0/0 [10/0] via 10.200.1.254, port1
```

Why the default route using port2 is not displayed in the output of the second command?

A. it has a lower priority than the default route using port1.
B. it has a higher priority than the default route using port1.
C. it has a higher distance than the default route using port1.
D. it is disabled in the FortiGate configuration.

Answer: A

QUESTION 5
An administrator has configured a dial-up IPsec VPN with one phase 2, extended authentication (XAuth) and IKE mode configuration. The administrator has also enabled the IKE real time debug.

```
diagnose debug applicationike -1
diagnose debug enable
```

In which order is each step and phase displayed in the debug output each time a new dial- up user is connecting to the VPN?

A. Phase 1; IKE mode configuration; XAuth; phase 2.
B. Phase 1; XAuth; IKE mode configuration; phase 2.
C. Phase 1; XAuth; phase 2, IKE mode configuration.
D. Phase 1; IKE mode configuration; phase 2; XAuth.

Answer: D

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.