DUMPSBOSS.COM

# Fortinet NSE 7 - Enterprise Firewall 6.2

## Fortinet NSE7_EFW-6.2

## Version Demo

**Total Demo Questions: 10**

**Total Premium Questions: 102**

**Buy Premium PDF**

https://dumpsboss.com

support@dumpsboss.com

## QUESTION NO: 1

View the exhibit, which contains the output of a BGP debug command, and then answer the question below.

```
# get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor     V     AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.125.0.60  4  65060     1698     1756     103    0     0  03:02:49             1
10.127.0.75  4  65075     2206     2250     102    0     0  02:45:55             1
10.200.3.1   4  65501      101      115       0    0     0  never              Active

Total number of neighbors 3
```

Which of the following statements about the exhibit are true? (Choose two.)

**A.** For the peer 10.125.0.60, the BGP state of is Established.

**B.** The local BGP peer has received a total of three BGP prefixes.

**C.** Since the BGP counters were last reset, the BGP peer 10.200.3.1 has never been down.

**D.** The local BGP peer has not established a TCP session to the BGP peer 10.200.3.1.

**ANSWER: A D**

## QUESTION NO: 2

A corporate network allows Internet Access to FSSO users only. The FSSO user student does not have Internet access after successfully logged into the Windows AD network. The output of the 'diagnose debug authd fsso list' command does not show student as an active FSSO user. Other FSSO users can access the Internet without problems. What should the administrator check? (Choose two.)

**A.** The user student must not be listed in the CA's ignore user list.

**B.** The user student must belong to one or more of the monitored user groups.

**C.** The student workstation's IP subnet must be listed in the CA's trusted list.

**D.** At least one of the student's user groups must be allowed by a FortiGate firewall policy.

**ANSWER: A D**

**Explanation:**

https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828

**QUESTION NO: 3**

View the exhibit, which contains the partial output of an IKE real-time debug, and then answer the question below.

```
ike 0:c49e59846861b0f6/0000000000000000:278: responder: main mode get 1st message...
ike 0:c49e59846861b0f6/0000000000000000:278: incoming proposal:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 0:
ike 0:c49e59846861b0f6/0000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:     trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:     encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_ENCRYPT_ALG, val=3DES_CBC.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: my proposal, gw VPN:
ike 0:c49e59846861b0f6/0000000000000000:278: proposal id = 1:
ike 0:c49e59846861b0f6/0000000000000000:278:   protocol id = ISAKMP:
ike 0:c49e59846861b0f6/0000000000000000:278:     trans_id = KEY_IKE.
ike 0:c49e59846861b0f6/0000000000000000:278:     encapsulation = IKE/none
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_ENCRYPT_ALG, val=AES_CBC,
key-len=256
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:c49e59846861b0f6/0000000000000000:278:       type=OAKLEY_GROUP, val=MODP2048.
ike 0:c49e59846861b0f6/0000000000000000:278: ISAKMP SA lifetime=86400
...
ike 0:c49e59846861b0f6/0000000000000000:278: negotiation failure
ike Negotiate ISAKMP SA Error: ike 0:c49e59846861b0f6/0000000000000000:278:
proposal chosen
...
```

Why didn't the tunnel come up?

**A.** The pre-shared keys do not match.

**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.** The remote gateway is using aggressive mode and the local gateway is configured to use man mode.

**ANSWER: C**

## QUESTION NO: 4

An administrator has configured the following CLI script on FortiManager, which failed to apply any changes to the managed device after being executed.

```
# conf rout stat
#    edit 0
#        set gateway 10.20.121.2
#        set priority 20
#        set device "wan1"
#    next
# end
```

Why didn't the script make any changes to the managed device?

**A.** Commands that start with the # sign are not executed.

**B.** CLI scripts will add objects only if they are referenced by policies.

**C.** Incomplete commands are ignored in CLI scripts.

**D.** Static routes can only be added using TCL scripts.

**ANSWER: A**

**Explanation:**

https://help.fortinet.com/fmgr/50hlp/56/5-6-2/FortiManager_Admin_Guide/1000_Device%20Manager/2400_Sc

A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.

## QUESTION NO: 5

A FortiGate device has the following LDAP configuration:

```
config user ldap
   edit "WindowsLDAP"
     set server "10.0.1.10"
     set cnid "cn"
     set dn "cn=user, dc=trainingAD, dc=training, dc=lab"
     set type regular
     set username "cn=administrator, cn=users, dc=trainingAD,
dc=training, dc=lab"
     set password xxxxx
   next
end
```

The LDAP user student cannot authenticate. The exhibit shows the output of the authentication real time debug while testing the student account:

```
#diagnose debug application fnbamd -1
#diagnose debug enable
#diagnose test authserver ldap WindowsLDAP student password
fnbamd_fsm.c[1819] handle_req-Rcvd auth req 4 for student in WindowsLDAP
opt=27 prot=0
fnbamd_fsm.c[336]_compose _group_list_from_req_Group 'WindowsLDAP'
fnbamd_pop3.c[573] fnband_pop3_start-student
fnbamd_cfg.c[932] fnbamd_cfg-get_ldap_:ist_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[1700] fnbamd_ldap_get_result-Error in ldap result: 49
(Invalid credentials)
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 4
fnbamd_fsm.c[568] destroy_auth_session-delete session 4
authenticate 'student' against 'WindowsLDAP' failed!
```

Based on the above output, what FortiGate LDAP settings must the administer check? (Choose two.)

**A.** cnid.

**B.** username.

**C.** password.

**D.** dn.

**ANSWER: B C**

**Explanation:**

https://kb.fortinet.com/kb/viewContent.do?externalId=13141

## QUESTION NO: 6

What is the purpose of an internal segmentation firewall (ISFW)?

**A.** It inspects incoming traffic to protect services in the corporate DMZ.

**B.** It is the first line of defense at the network perimeter.

**C.** It splits the network into multiple security segments to minimize the impact of breaches.

**D.** It is an all-in-one security appliance that is placed at remote sites to extend the enterprise network.

**ANSWER: C**

**Explanation:**

ISFW splits your network into multiple security segments. They serve as a breach containers from attacks that come from inside.

## QUESTION NO: 7

View the exhibit, which contains the output of a debug command, and then answer the question below.

```
# get router info ospf interface port4
port4 is up, line protocol is up
   Internet Address 172.20.121.236/24, Area 0.0.0.0, MTU 1500
   Process ID 0, Router ID 0.0.0.4, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State DROther, Priority 1
   Designated Router (ID) 172.20.140.2, Interface Address 172.20.121.2
Backup Designated Router (ID) 0.0.0.1, Interface Address 172.20.121.239
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:05
   Neighbor Count is 4, Adjacent neighbor count is 2
   Crypt Sequence Number is 411
   Hello received 106, sent 27, DD received 7 sent 9
   LS-Req received 2 sent 2, LS-Upd received 7 sent 5
   LS-Ack received 4 sent 3, Discarded 1
```

Which of the following statements about the exhibit are true? (Choose two.)

**A.** In the network on port4, two OSPF routers are down.

**B.** Port4 is connected to the OSPF backbone area.

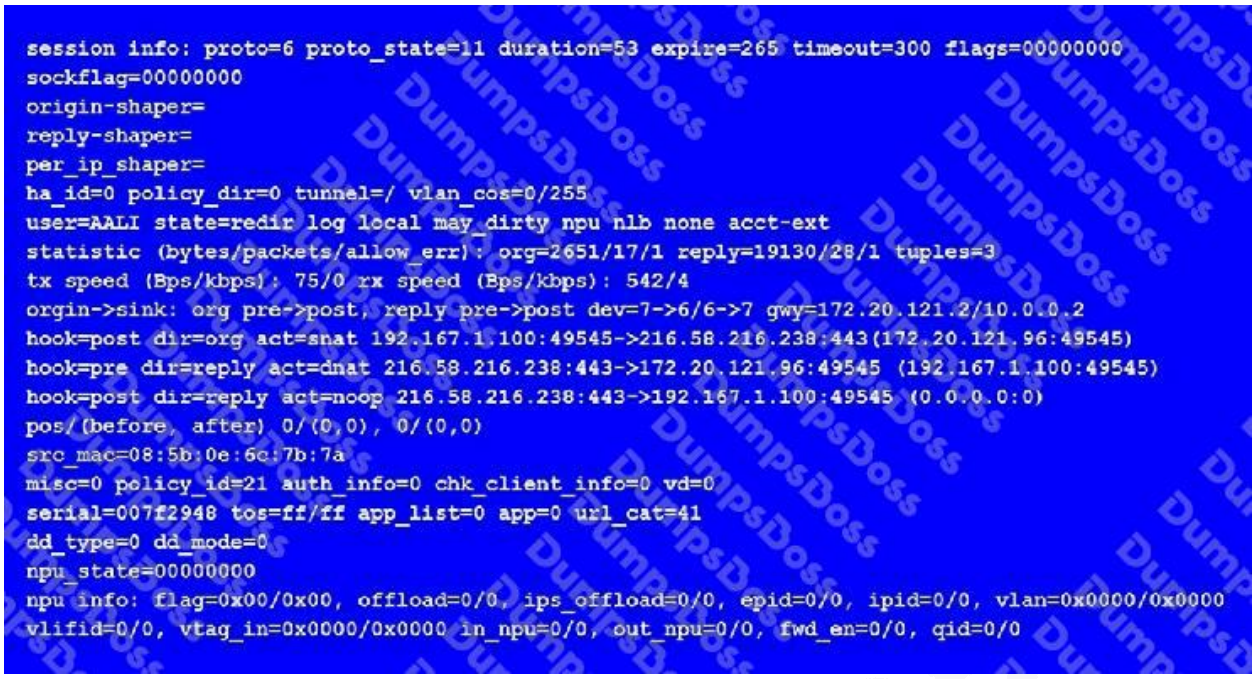
**C.** The local FortiGate's OSPF router ID is 0.0.0.4

**D.** The local FortiGate has been elected as the OSPF backup designated router.

**ANSWER: B C**

## QUESTION NO: 8

View the exhibit, which contains an entry in the session table, and then answer the question below.




Which one of the following statements is true regarding FortiGate's inspection of this session?

**A.** FortiGate applied proxy-based inspection.

**B.** FortiGate forwarded this session without any inspection.

**C.** FortiGate applied flow-based inspection.

**D.** FortiGate applied explicit proxy-based inspection.

**ANSWER: A**

**Explanation:**

https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

## QUESTION NO: 9

Which statements about bulk configuration changes using FortiManager CLI scripts are correct? (Choose

two.)

**A.** When executed on the Policy Package, ADOM database, changes are applied directly to the managed FortiGate.

**B.** When executed on the Device Database, you must use the installation wizard to apply the changes to the managed FortiGate.

**C.** When executed on the All FortiGate in ADOM, changes are automatically installed without creating a new revision history.

**D.** When executed on the Remote FortiGate directly, administrators do not have the option to review the changes prior to installation.

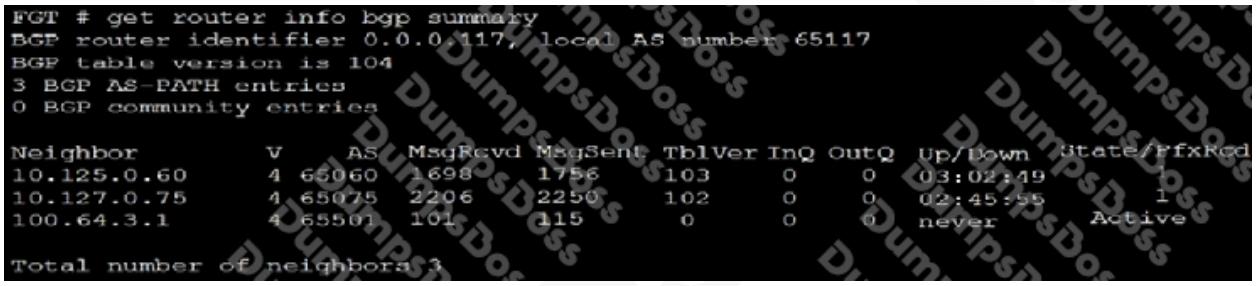
**ANSWER: B D**

**Explanation:**

CLI scripts can be run in three different ways:Device Database: By default, a script is executed on the device database. It is recommend you run the changes on the device database (default setting), as this allows you to check what configuration changes you will send to the managed device. Once scripts are run on the device database, you can install these changes to a managed device using the installation wizard.

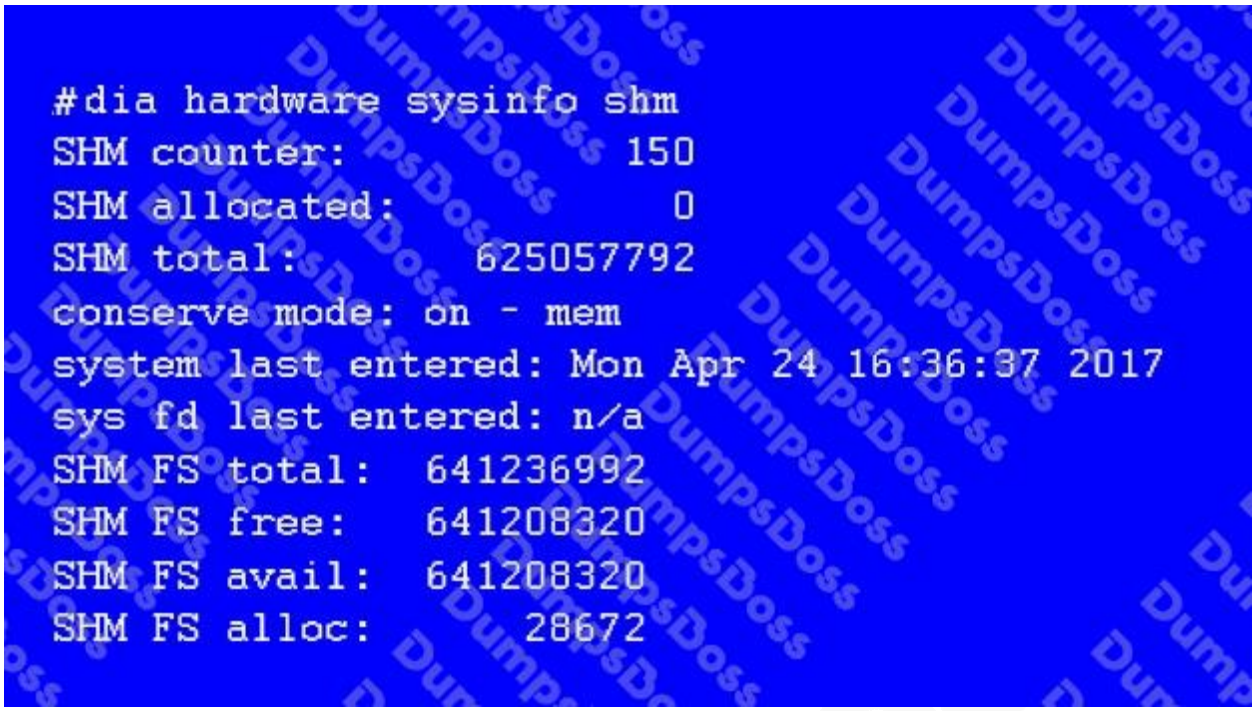
Policy Package, ADOM database: If a script contains changes related to ADOM level objects and policies, you can change the default selection to run on Policy Package, ADOM database and can then be installed using the installation wizard.

Remote FortiGate directly (through CLI): A script can be executed directly on the device and you don't need to install these changes using the installation wizard. As the changes are directly installed on the managed device, no option is provided to verify and check the configuration changes through FortiManager prior to executing it.




**QUESTION NO: 10**

View the exhibit, which contains the output of a debug command, and then answer the question below.




What statement is correct about this FortiGate?

**A.** It is currently in system conserve mode because of high CPU usage.

**B.** It is currently in FD conserve mode.

**C.** It is currently in kernel conserve mode because of high memory usage.

**D.** It is currently in system conserve mode because of high memory usage.

**ANSWER: D**