



NSE7^{Q&As}

Fortinet Troubleshooting Professional

Pass Fortinet NSE7 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/nse7.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

Examine the output from the BGP real time debug shown in the exhibit, then the answer the question below:

```
# diagnose ip router bgp all enable
# diagnose ip router bgp level info
# diagnose debug enable
"BGP: 10.200.3.1-Outgoing [DECODE] KAlive: Received!"
"BGP: 10.200.3.1-Outgoing [FSM] State: OpenConfirm Event: 26"
"BGP: 10.200.3.1-Outgoing [DECODE] Msg-Hdr: type 2, length 56"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: Starting UPDATE decoding... Byt
(37), msg_size (37)"
"BGP: 10.200.3.1-Outgoing [DECODE] Update: NLRI Len(13)"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 27"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 0.0.0.0/0"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.4.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.200.3.0/24"
"BGP: 10.200.3.1-Outgoing [RIB] Update: Received Prefix 10.0.2.0/24"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
"BGP: 10.200.3.1-Outgoing [ENCODE] Msg-Hdr: Type 2"
"BGP: 10.200.3.1-Outgoing [ENCODE] Attr IP-Unicast: Tot-attr-len 20"
"BGP: 10.200.3.1-Outgoing [ENCODE] Update: Msg #5 Size 55"
"BGP: 10.200.3.1-Outgoing [FSM] State: Established Event: 34"
```

Which statements are true regarding the output in the exhibit? (Choose two.)

- A. BGP peers have successfully interchanged Open and Keepalive messages.
- B. Local BGP peer received a prefix for a default route.
- C. The state of the remote BGP peer is OpenConfirm.
- D. The state of the remote BGP peer will go to Connect after it confirms the received prefixes.

Correct Answer: AB

QUESTION 2

Examine the output from the `\\diagnose debug authd fsso list\\` command; then answer the question below.

```
# diagnose debug authd fsso list --FSSO logons-IP: 192.168.3.1 User: STUDENT Groups: TRAININGAD/
USERS Workstation: INTERNAL2. TRAINING. LAB The IP address 192.168.3.1 is NOT the one used by
the workstation INTERNAL2. TRAINING.
LAB.
```

What should the administrator check?

- A. The IP address recorded in the logon event for the user STUDENT.
- B. The DNS name resolution for the workstation name INTERNAL2. TRAINING. LAB.
- C. The source IP address of the traffic arriving to the FortiGate from the workstation INTERNAL2. TRAINING. LAB.



D. The reserve DNS lookup for the IP address 192.168.3.1.

Correct Answer: C

QUESTION 3

A FortiGate device has the following LDAP configuration: The LDAP user student cannot authenticate. The exhibit shows the output of the authentication real time debug while testing the student account:

```
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
```

```
#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] 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[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 administrator check? (Choose two.)

- A. cnid.
- B. username.
- C. password.
- D. dn.

Correct Answer: BC

QUESTION 4

View the exhibit, which contains a session entry, and then answer the question below.

```
session info: proto=1 proto_state=00 duration=1 expire=59 timeout=0 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=log may_dirty none
statistic(bytes/packets/allow_err): org=168/2/1 reply=168/2/1 tuples=2
tx speed(Bps/kbps): 97/0 rx speed(Bps/kbps): 97/0
origin->sink: org pre->post, reply pre->post dev=9->3/3->9 gwy=10.200.1.254/10.1.0.1
hook=post dir=org act=snat 10.1.10.10:40602->10.200.5.1:8(10.200.1.254/10.1.0.1
hook=pre dir=reply act=dnat 10.200.5.1:60430->10.200.1.1:0(10.1.10.10:40602)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=0002a5c9 tos=ff/ff app_list=0 app=0 url_cat=0
dd_type=0 dd_mode=0
```

Which statement is correct regarding this session?

- A. It is an ICMP session from 10.1.10.10 to 10.200.1.1.
- B. It is an ICMP session from 10.1.10.10 to 10.200.5.1.
- C. It is a TCP session in ESTABLISHED state from 10.1.10.10 to 10.200.5.1.
- D. It is a TCP session in CLOSE_WAIT state from 10.1.10.10 to 10.200.1.1.

Correct Answer: A

QUESTION 5

Which of the following statements are true about FortiManager when it is deployed as a local FDS? (Choose two.)

- A. Caches available firmware updates for unmanaged devices.
- B. Can be configured as an update server, or a rating server, but not both.



C. Supports rating requests from both managed and unmanaged devices.

D. Provides VM license validation services.

Correct Answer: AD

QUESTION 6

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

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7.... ike 0: IKEv1 exchange=Aggressive  
id=baf47d0988e9237f/2f405ef3952f6fda len=430 ike 0: in
```

```
BAF47D0988E9237F2F405EF3952F6FDA0110040000000000000001AE0400003C00000  
00100000001000000300101000 ike 0:RemoteSite:4: initiator: aggressive mode get 1st response... ike 0:RemoteSite:4:  
VID RFC 3947 4A131c81070358455C5728F20E95452F ike 0:RemoteSite:4: VID DPD  
AFCAD71368A1F1C96B8696FC77570100 ike 0:RemoteSite:4: VID FORTIGATE  
8299031757A36082C6A621DE000502D7 ike 0:RemoteSite:4: peer is FortiGate/Fortios (v5 b727)
```

```
ike 0:RemoteSite:4: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3 ike 0:RemoteSite:4: VID  
FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
```

```
ike 0:RemoteSite:4: received peer identifier FQDN `remote\`
```

```
ike 0:RemoteSite:4: negotiation result
```

```
ike 0:RemoteSite:4: proposal id = 1:
```

```
ike 0:RemoteSite:4: protocol id = ISAKMP:
```

```
ike 0:RemoteSite:4: trans_id = KEY_IKE.
```

```
ike 0:RemoteSite:4: encapsulation = IKE/none
```

```
ike 0:RemoteSite:4: type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key ?en=128
```

```
ike 0:RemoteSite:4: type=OAKLEY_HASH_ALG, val=SHA.
```

```
ike 0:RemoteSite:4: type=AUTH_METHOD, val=PRESHARED_KEY.
```

```
ike 0:RemoteSite:4: type=OAKLEY_GROUP, val=MODP1024.
```

```
ike 0:RemoteSite:4: ISAKMP SA lifetime=86400
```

```
ike 0:RemoteSite:4: ISAKMP SA baf47d0988e9237f/2f405ef3952f6fda key 16:
```

```
B25B6C9384D8BDB24E3DA3DC90CF5E73
```

```
ike 0:RemoteSite:4: PSK authentication succeeded
```

```
ike 0:RemoteSite:4: authentication OK
```

```
ike 0:RemoteSite:4: add INITIAL-CONTACT
```

```
ike 0:RemoteSite:4: enc BAF47D0988E9237F405EF3952F6FDA081004010000000000000080140000181F2E48BF
```



D8E9D603F ike 0:RemoteSite:4: out

BAF47D0988E9237F405EF3952F6FDA081004010000000000000008C2E3FC9BA061816A 396F009A12

ike 0:RemoteSite:4: sent IKE msg (agg_i2send): 10.0.0.1:500-10.0.0.2:500, len=140, id=baf47d0988e9237f/2 ike 0:RemoteSite:4: established IKE SA baf47d0988e9237f/2f405ef3952f6fda

Which statements about this debug output are correct? (Choose two.)

- A. The remote gateway IP address is 10.0.0.1.
- B. It shows a phase 1 negotiation.
- C. The negotiation is using AES128 encryption with CBC hash.
- D. The initiator has provided remote as its IPsec peer ID.

Correct Answer: BD

QUESTION 7

Which of the following statements is true regarding a FortiGate configured as an explicit web proxy?

- A. FortiGate limits the number of simultaneous sessions per explicit web proxy user. This limit CANNOT be modified by the administrator.
- B. FortiGate limits the total number of simultaneous explicit web proxy users.
- C. FortiGate limits the number of simultaneous sessions per explicit web proxy user The limit CAN be modified by the administrator
- D. FortiGate limits the number of workstations that authenticate using the same web proxy user credentials. This limit CANNOT be modified by the administrator.

Correct Answer: C

QUESTION 8

What global configuration setting changes the behavior for content-inspected traffic while FortiGate is in system conserve mode?

- A. av-failopen
- B. mem-failopen
- C. utm-failopen
- D. ips-failopen

Correct Answer: A

**QUESTION 9**

A FortiGate is rebooting unexpectedly without any apparent reason. What troubleshooting tools could an administrator use to get more information about the problem? (Choose two.)

- A. Firewall monitor.
- B. Policy monitor.
- C. Logs.
- D. Crashlogs.

Correct Answer: CD

QUESTION 10

Examine the output from the `diagnose vpn tunnel list` command shown in the exhibit; then answer the question below.

```
#diagnose vpn tunnel list
name=Dial Up_0 ver=1 serial=5 10.200.1.1:4500->10.200.3.2: 64916 lgwy=static
nun=intf mode=dial_inst.bound if=2
parent=DialUp index=0
proxyid_um=1 child_num=0 refcnt=8 ilast=4 olast=4
stat: rxp=104 txp=8 rxb=27392 txb=480
dpd: mode=active on=1 idle=5000ms retry=3 count=0 segno=70
natt: mode=silent draft=32 interval= 10 remote_port=64916
proxyid= DialUp proto=0 sa=1 ref=2 serial=1 add-route
src: 0:0.0.0.0.-255.255.255.255:0
dst: 0:10.0.10.10.-10.0.10.10:0
SA: ref=3 options= 00000086 type=00 soft=0 mtu=1422 expire =42521
replaywin=2048 seqno=9
life: type=01 bytes=0/0 timeout= 43185/43200
dec: spi=cb3a632a esp=aes key=16 7365e17a8fd555ec38bffa47d650c1a2
    ah=sha1 key=20 946bfb9d23b8b53770dcf48ac2af82b8ccc6aa85
enc: spi=da6d28ac esp=aes key=16 3dcf44ac7c816782ea3d0c9a977ef543
    ah=sha1 key=20 7cfde587592fc4635ab8db8ddf0d851d868b243f
dec:pkts/bytes=104/19926, enc:pkts/bytes=8/1024
```

Which command can be used to sniff the ESP traffic for the VPN DialUP_0?



- A. diagnose sniffer packet any `port 500\\`
- B. diagnose sniffer packet any `esp\\`
- C. diagnose sniffer packet any `host 10.0.10.10\\`
- D. diagnose sniffer packet any `port 4500\\`

Correct Answer: B

QUESTION 11

View the following FortiGate configuration.

```
config system global
    set snat-route-change disable
end
config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

All traffic to the Internet currently egresses from port1. The exhibit shows partial session information for Internet traffic from a user on the internal network:



```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=17 expire=7 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
ha_id=0 policy_dir=0 tunnel=/
state=may_dirty none app_ntf
statistic(bytes/packets/allow_err): org=57555/7/1 reply=23367/19/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907-
>54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80-
>10.200.1.1:64907(10.0.1.10:64907)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000294 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the priority on route ID 1 were changed from 5 to 20, what would happen to traffic matching that user's session?

- A. The session would remain in the session table, and its traffic would still egress from port1.
- B. The session would remain in the session table, but its traffic would now egress from both port1 and port2.
- C. The session would remain in the session table, and its traffic would start to egress from port2.
- D. The session would be deleted, so the client would need to start a new session.

Correct Answer: D

QUESTION 12

Examine the output of the `diagnose sys session list expectation` command shown in the exhibit; then answer the question below.



```
#diagnose sys session list expectation
```

```
session info: proto= proto_state=0 0 duration=3 expire=26 timeout=3600
flags=00000000
sockflag=.00000000.sockport=0.av_idx=0.use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0.policy_dir=1.tunnel=
state=new complex
statistic (bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
origin-> sink: org pre-> post, reply pre->post dev=2->4/4->2
gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0-> 10.200.1.1: 60426
(10.0.1.10: 50365)
hook= pre dir=org act=noop 0.0.0.0.:0-> 0.0.0.0:0 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
misc=0.policy_id=1.auth_info=0.chk_client_info=0.vd=0
seriall=000000e9.tos=ff/ff.ips_view=0 app_list=0.app=0
dd type=0.dd_mode=0
```

Which statement is true regarding the session in the exhibit?

- A. It was created by the FortiGate kernel to allow push updates from FortiGuard.
- B. It is for management traffic terminating at the FortiGate.
- C. It is for traffic originated from the FortiGate.
- D. It was created by a session helper or ALG.

Correct Answer: A

QUESTION 13

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.

Correct Answer: BC

QUESTION 14

Which of the following statements are correct regarding application layer test commands? (Choose two.)

- A. They are used to filter real-time debugs.
- B. They display real-time application debugs.
- C. Some of them display statistics and configuration information about a feature or process.
- D. Some of them can be used to restart an application.

Correct Answer: BC

QUESTION 15

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=Users, dc=trainingAD, dc=training, dc=lab"
    set type regular
    set username "dc=trainingAD, dc=training, dc=lab"
    set password xxxxxxxx
  next
end
```

The administrator executed the `dsquery\\` command in the Windows LDAP server 10.0.1.10, and got the following output:

```
>dsquery user -samid administrator
```

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

Based on the output, what FortiGate LDAP setting is configured incorrectly?

- A. cnid.
- B. username.
- C. password.
- D. dn.

Correct Answer: A

[Latest NSE7 Dumps](#)

[NSE7 VCE Dumps](#)

[NSE7 Study Guide](#)