



# NSE7\_EFW-6.4<sup>Q&As</sup>

Fortinet NSE 7 - Enterprise Firewall 6.4

## Pass Fortinet NSE7\_EFW-6.4 Exam with 100% Guarantee

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

[https://www.passapply.com/nse7\\_efw-6-4.html](https://www.passapply.com/nse7_efw-6-4.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

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

```
session info: proto=6 proto_state=11 duration=53 expire=265 timeout=300 flags=00000000
sockflag=00000000
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
user=AALI state=redir log local may_dirty npu nlb none acct-ext
statistic (bytes/packets/allow_err): org=2651/17/1 reply=19130/28/1 tuples=3
tx speed (Bps/kbps): 75/0 rx speed (Bps/kbps): 542/4
orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.20.121.2/10.0.0.2
hook=post dir=org act=snat 192.167.1.100:49545->216.58.216.238:443 (172.20.121.96:49545)
hook=pre dir=reply act=dnat 216.58.216.238:443->172.20.121.96:49545 (192.167.1.100:49545)
hook=post dir=reply act=noop 216.58.216.238:443->192.167.1.100:49545 (0.0.0.0:0)
pos/(before, after) 0/(0,0), 0/(0,0)
src_mac=08:5b:0e:6c:7b:7a
misc=0 policy_id=21 auth_info=0 chk_client_info=0 vd=0
serial=007f2948 tos=ff/ff app_list=0 app=0 url_cat=41
dd_type=0 dd_mode=0
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
```

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.

Correct Answer: A

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

## QUESTION 2

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: B

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD37516>

---

### QUESTION 3

An administrator is running the following sniffer in a FortiGate:

```
diagnose sniffer packet any "host 10.0.2.10" 2
```

What information is included in the output of the sniffer? (Choose two.)

- A. Ethernet headers.
- B. IP payload.
- C. IP headers.
- D. Port names.

Correct Answer: BC



<https://kb.fortinet.com/kb/documentLink.do?externalID=11186>

---

#### QUESTION 4

Which two conditions must be met for a statistic route to be active in the routing table? (Choose two.)

- A. The link health monitor (if configured) is up.
- B. There is no other route, to the same destination, with a higher distance.
- C. The outgoing interface is up.
- D. The next-hop IP address is up.

Correct Answer: AC

---

#### QUESTION 5

Two independent FortiGate HA clusters are connected to the same broadcast domain. The administrator has reported that both clusters are using the same HA virtual MAC address. This creates a duplicated MAC address problem in the network. What HA setting must be changed in one of the HA clusters to fix the problem?

- A. Group ID.
- B. Group name.
- C. Session pickup.
- D. Gratuitous ARPs.

Correct Answer: A

[https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA\\_failoverVMAC.htm](https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_failoverVMAC.htm)

---

#### QUESTION 6

Refer to the exhibit, which shows a partial routing table.



```
FGT # get router info routing-table all
...
Routing table for VRF=7
C    10.73.9.0/24 is directly connected, port2

Routing table for VRF=12
C    10.1.0.0/24 is directly connected, port3
S    10.10.4.0/24 [10/0] via 10.1.0.100, port3
C    10.64.1.0/24 is directly connected, port1

Routing table for VRF=21
S    10.1.0.0/24 [10/0] via 10.72.3.254, port4
C    10.72.3.0/24 is directly connected, port4
```

Assuming all the appropriate firewall policies are configured, which two pings will FortiGate route? (Choose two.)

- A. Source IP address: 10.1.0.10. Destination IP address: 10.64.1.52
- B. Source IP address: 10.72.3.52. Destination IP address: 10.1.0.254
- C. Source IP address: 10.10.4.24, Destination IP address: 10.72.3.20
- D. Source IP address: 10.73.9.10, Destination IP address: 10.72.3.15

Correct Answer: AB

## QUESTION 7

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

```
Spoke-2 # dia vpn tunnel list
list all ipsec tunnel in vd 0
name=VPN ver=1 serial=1 10.200.5.1:0->10.200.4.1:0
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=10 olast=792 auto-discovery=0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000 ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=VPN proto=0 sa=1 ref=2 serial=1
src: 0:10.1.2.0/255.255.0:0
dst: 0:10.1.1.0/255.255.255.0:0
SA: ref=3 options=2e type=00 soft=0 mtu=1438 expire=42403/0B replaywin=2048 seqno=1 esn=0
replaywin_lastseq=00000000
life: type=01 bytes=0/0 timeout=43177/43200
dec: spi=ccc1f66d esp=aes key=16 280e5cd6f9bacc65ac771556c464ffbd
ah=shal key=20 c68091d68753578785de6a7a6b276b506c527efe
enc: spi=df14200b esp=aes key=16 b02a7e9f5542b69aff6aa391738ee393
ah=shal key20 889f7529887c215c25950be2ba83e6fela5367be
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```



Based on the output, which of the following statements is correct?

- A. Anti-reply is enabled.
- B. DPD is disabled.
- C. Quick mode selectors are disabled.
- D. Remote gateway IP is 10.200.5.1.

Correct Answer: A

### QUESTION 8

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

```
# diagnose debug rating
Locale      : english
License     : Contract
Expiration  : Thu Sep 28 17:00:00 20xx
== Server List (Thu Apr 19 10:41:32 20xx) ==
IP          Weight  RTT   Flags  TZ   Packets  Curr Lost  Total Lost
64.26.151.37  10     45    -5     -5   262432   0          846
64.26.151.35  10     46    -5     -5   329072   0          6806
66.117.56.37  10     75    -5     -5   71638    0          275
65.210.95.240 20     71    -8     -8   36875    0          92
209.222.147.36 20     103   DI     -8   34784    0          1070
208.91.112.194 20     107   D      -8   35170    0          1533
96.45.33.65   60     144   0      0    33728    0          120
80.85.69.41   71     226   1      1    33797    0          192
62.209.40.74  150    97    9      9    33754    0          145
121.111.236.179 45     44    F      -5   26410    26226     26227
```

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

- A. FortiGate will probe 121.111.236.179 every fifteen minutes for a response.
- B. Servers with the D flag are considered to be down.
- C. Servers with a negative TZ value are experiencing a service outage.
- D. FortiGate used 209.222.147.3 as the initial server to validate its contract.

Correct Answer: AD



### QUESTION 9

Refer to exhibit, which contains the output of a BGP debug command.

```
FGT # get router info bgp summary
BGP router identifier 10.200.1.1, local AS number 65501
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor      V    AS      MsgRcvd MsgSent   TblVer.
10.200.3.1    4  65501    92      1756     0

Total number of neighbors 1
```

Which statement explains why the state of the 10.200.3.1 peer is Connect?

- A. The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the OpenConfirm yet.
- B. The TCP session to 10.200.3.1 has not completed the three-way handshake.
- C. The local router is receiving the BGP keepalives from the peer, but it has not received a BGP prefix yet.
- D. The local router has received the BGP prefixes from the remote peer.

Correct Answer: B

### QUESTION 10

Which statement about the designated router (DR) and backup designated router (BDR) in an OSPF multi-access network is true?

- A. FortiGate first checks the OSPF ID to elect a DR.
- B. Non-DR and non-BDR routers will form full adjacencies to DR and BDR only.
- C. BDR is responsible for forwarding link state information from one router to another.
- D. Only the DR receives link state information from non-DR routers.

Correct Answer: B

### QUESTION 11

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 fssolist` 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.

Correct Answer: AD

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

## QUESTION 12

Refer to the exhibit, which contains partial output from an IKE real-time debug.

```
ike 0: comes 10.0.0.2:500->10.0.0.1:500, ifindex=7. . . .
ike 0: IKEv2 exchange=Aggressive id=a2fbd6bb6394401a/06b89c022d4df682 len=426
ike 0: Remotesite:3: initiator: aggressive mode get 1st response. . .
ike 0: Remotesite:3: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0: Remotesite:3: DPD negotiated
ike 0: Remotesite:3: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0: Remotesite:3: peer is FortiGate/FortiOS (v0 b0)
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0: Remotesite:3: received peer identifier FQDN 'remote'
ike 0: Remotesite:3: negotiation result
ike 0: Remotesite:3: proposal id = 1:
ike 0: Remotesite:3:     protocol id = ISAKMP:
ike 0: Remotesite:3:         trans_id = KEY_IKE.
ike 0: Remotesite:3:         encapsulation = IKE/none.
ike 0: Remotesite:3:             type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0: Remotesite:3:             type=OAKLEY_HASH_ALG, val=SHA.
ike 0: Remotesite:3:             type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0: Remotesite:3:             type=OAKLEY_GROUP, val=MODP1024.
ike 0: Remotesite:3: ISAKMP SA lifetime=86400
ike 0: Remotesite:3: NAT-T unavailable
ike 0: Remotesite:3: ISAKMP SA a2fbd6bb6394401a/06b89c022d4df682 key
16:39915120ED73ED73E520787C801DE3678916
ike 0: Remotesite:3: PSK authentication succeeded
ike 0: Remotesite:3: authentication OK
ike 0: Remotesite:3: add INITIAL-CONTACT
ike 0: Remotesite:3: enc
A2FBD6BB6394401A06B89C022D4DF682081004010000000000000500B000018882A07BE09026CA8B2
ike 0: Remotesite:3: out
A2FBD6BB6394401A06B89C022D4DF6820810040100000000000005C64D5CBA90B873F150CB8B5CC2A
ike 0: Remotesite:3: sent IKE msg (agg_i2send): 10.0.0.1:500->10.0.0.2:500, len=140,
id=a2fbd6bb6394401a/
ike 0: Remotesite:3: established IKE SA a2fbd6bb6394401a/06b89c022d4df682
```

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





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

Correct Answer: BC

### QUESTION 13

Examine the output of the `get router info ospf neighbor` command shown in the exhibit; then answer the question below.

```
# get router info ospf neighbor
```

```
OSPF process 0:
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
0.0.0.69	1	Full/DR	00:00:32	10.126.0.69	wan1
0.0.0.117	1	Full/DROther	00:00:34	10.126.0.117	wan1
0.0.0.2	1	Full/ -	00:00:36	172.16.1.2	ToRemote

Refer to the exhibit, which shows the output of a debug command.

Which statement about the output is true?

- A. The OSPF routers with the IDs 0.0.0.69 and 0.0.0.117 are both designated routers for the wan1 network.
- B. The OSPF router with the ID 0.0.0.2 is the designated router for the ToRemote network.
- C. The local FortiGate is the designated router for the wan1 network.
- D. The interface ToRemote is a point-to-point OSPF network.

Correct Answer: D

<https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13685-13.html>

### QUESTION 14

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/. [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.

Correct Answer: C

<http://kb.fortinet.com/kb/viewContent.do?externalId=FD32103>

#### QUESTION 15

What does the dirty flag mean in a FortiGate session?

- A. Traffic has been blocked by the antivirus inspection.
- B. The next packet must be re-evaluated against the firewall policies.
- C. The session must be removed from the former primary unit after an HA failover.
- D. Traffic has been identified as from an application that is not allowed.

Correct Answer: B

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD40119andslicId=1>

[Latest NSE7\\_EFW-6.4 Dumps](#)

[NSE7\\_EFW-6.4 PDF Dumps](#)

[NSE7\\_EFW-6.4 Practice Test](#)