

# DumpsCafe

## Fortinet

### NSE7\_EFW-7.0



Fortinet NSE 7 -  
Enterprise Firewall 7.0

**Version: Demo**

[ Total Questions: 10]

Web: [www.dumpscafe.com](http://www.dumpscafe.com)

Email: [support@dumpscafe.com](mailto:support@dumpscafe.com)

# IMPORTANT NOTICE

## Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at [feedback@dumpsafe.com](mailto:feedback@dumpsafe.com)

## Support

If you have any questions about our product, please provide the following items:

- ➔ exam code
- ➔ screenshot of the question
- ➔ login id/email

please contact us at [support@dumpsafe.com](mailto:support@dumpsafe.com) and our technical experts will provide support within 24 hours.

## Copyright

The product of each order has its own encryption code, so you should use it independently. Any unauthorized changes will inflict legal punishment. We reserve the right of final explanation for this statement.

**Question #:1**

View the exhibit, which contains the output of diagnose sys session list, and then answer the question below.

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 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=0 tunnel=/
state=may_dirty synced none app_ntf
statistic (bytes/packets/allow_err): org=822/11/1 reply=9037/15/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4 gw=10.200.1.254/10.0.1.10
hook=post dir=org act=snst 10.0.1.10:65464->54.192.15.182:80 (10.200.1.1:65464)
hook-pre dir=reply act=dnat 54.192.15.182:80->10.200.1.1:65464 (10.0.1.10:65464)
pos/ (before, after) 0/(0/0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary unit is zero (0), which statement is correct regarding the output?

- A. This session is for HA heartbeat traffic.
- B. This session is synced with the slave unit.
- C. The inspection of this session has been offloaded to the slave unit.
- D. This session cannot be synced with the slave unit.

**Answer: B**

**Question #:2**

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
A2FBD6BB6394401A06B89C022D4DF6820810040100000000000000500B000018882A07BE09026CA8B2
ike 0: Remotesite:3: out
A2FBD6BB6394401A06B89C022D4DF68208100401000000000000005C64D5CBA90B873F150CB8B5CC2A
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.

**Answer: B C**

**Question #3**

Examine the following routing table and BGP configuration; then answer the question below.

```
#get router info routing-table all
*0.0.0.0/0 [10/0] via 10.200.1.254, port1
C10.200.1.0/24 is directly connected, port1
S192.168.0.0/16 [10/0] via 10.200.1.254, port1
# show router bgp
config router bgp
set as 65500
set router-id 10.200.1.1
set network-import-check enable
set ebgp-multipath disable
config neighbor
edit "10.200.3.1"
set remote-as 65501
next
end
config network
edit1
```

The BGP connection is up, but the local peer is NOT advertising the prefix 192.168.1.0/24. Which configuration change will make the local peer advertise this prefix?

- A. Enable the redistribution of connected routers into BGP.
- B. Enable the redistribution of static routers into BGP.
- C. Disable the setting network-import-check.
- D. Enable the setting ebgp-multipath.

**Answer: C**

**Question #4**

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 application ike-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. Phase1; IKE mode configuration; XAuth; phase 2.

- B. Phase1; XAuth; IKE mode configuration; phase2.
- C. Phase1; XAuth; phase 2; IKE mode configuration.
- D. Phase1; IKE mode configuration; phase 2; XAuth.

**Answer: B**

### **Explanation**

[https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec\\_VPN\\_Concepts/IKE\\_Packet](https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/IKE_Packet)

#### **Question #:5**

How does FortiManager handle FortiGuard requests from FortiGate devices, when it is configured as a local FDS?

- A. FortiManager can download and maintain local copies of FortiGuard databases.
- B. FortiManager supports only FortiGuard push to managed devices.
- C. FortiManager will respond to update requests only if they originate from a managed device.
- D. FortiManager does not support rating requests.

**Answer: A**

#### **Question #: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 #: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 #:8**

An administrator has configured two FortiGate devices for an HA cluster. While testing the HA failover, the administrator noticed that some of the switches in the network continue to send traffic to the former primary unit. The administrator decides to enable the setting link-failed-signal to fix the problem. Which statement is correct regarding this command?

- A. Forces the former primary device to shut down all its non-heartbeat interfaces for one second while the failover occurs.
- B. Sends an ARP packet to all connected devices, indicating that the HA virtual MAC address is reachable through a new master after a failover.
- C. Sends a link failed signal to all connected devices.
- D. Disables all the non-heartbeat interfaces in all the HA members for two seconds after a failover.

**Answer: A**

**Question #:9**

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

```
FGT # 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
100.64.3.1    4  65501    101      115     0     0    0   never        Active

Total number of neighbors 3
```

Which statement about the exhibit is true?

- A. The local router has received a total of three BGP prefixes from all peers.
- B. The local router has not established a TCP session with 100.64.3.1.
- C. Since the counters were last reset, the 10.200.3.1 peer has never been down.
- D. The local router BGP state is OpenConfirm with the 10.127.0.75 peer.

**Answer: B**

**Question #:10**

Refer to the exhibits.



```
config vpn ipsec phase1-interface
edit "user-1"
  set type dynamic
  set interface "port1"
  set mode main
  set xauthtype auto
  set authusrgrp "Users-1"
  set peertype any
  set dhgrp 14 15 19
  set proposal aes128-sha256 aes256-sha384
  set psksecret <encrypted_password>
next
```

Which contain the partial configurations of two VPNs on FortiGate.

An administrator has configured two VPNs for two different user groups. Users who are in the Users-2 group are not able to connect to the VPN. After running a diagnostics command, the administrator discovered that FortiGate is not matching the user-2 VPN for members of the Users-2 group.

Which two changes must administrator make to fix the issue? (Choose two.)

- A. Use different pre-shared keys on both VPNs
- B. Enable Mode Config on both VPNs.
- C. Set up specific peer IDs on both VPNs.
- D. Change to aggressive mode on both VPNs.

**Answer: C D**

# About [dumpsafe.com](http://dumpsafe.com)

[dumpsafe.com](http://dumpsafe.com) was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: [All vendors](#)

**Microsoft**



**CITRIX**



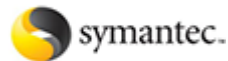
**(ISC)<sup>2</sup>**



**JUNIPER**  
NETWORKS



**ORACLE**



**vmware**

We prepare state-of-the-art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- ➔ Sales: [sales@dumpsafe.com](mailto:sales@dumpsafe.com)
- ➔ Feedback: [feedback@dumpsafe.com](mailto:feedback@dumpsafe.com)
- ➔ Support: [support@dumpsafe.com](mailto:support@dumpsafe.com)

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.