

DUMPSQUEEN

Fortinet NSE 7 - Enterprise Firewall 7.0

Fortinet NSE7 EFW-7.0

Version Demo

Total Demo Questions: 10

Total Premium Questions: 163

Buy Premium PDF

<https://dumpsqueen.com>

support@dumpsqueen.com

dumpsqueen.com

QUESTION NO: 1

Which the following events can trigger the election of a new primary unit in a HA cluster? (Choose two.)

- A. Primary unit stops sending HA heartbeat keepalives.
- B. The FortiGuard license for the primary unit is updated.
- C. One of the monitored interfaces in the primary unit is disconnected.
- D. A secondary unit is removed from the HA cluster.

ANSWER: A C

QUESTION NO: 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 4048B7D56EBC88525E7DE7F00D6C2D3
ike 0: Remotesite:3: VID FRAGMENTATION 4048B7D56EBC88525E7DE7F00D6C2D3C0000000
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
16:39915120ED73ED73E520787C8D1DE3678916
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
A2FBD6BB6394401A06B89C022D4DF6820810040100000000000000500C64D3CBA90B873F150CB8B5CC2A
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 NO: 3

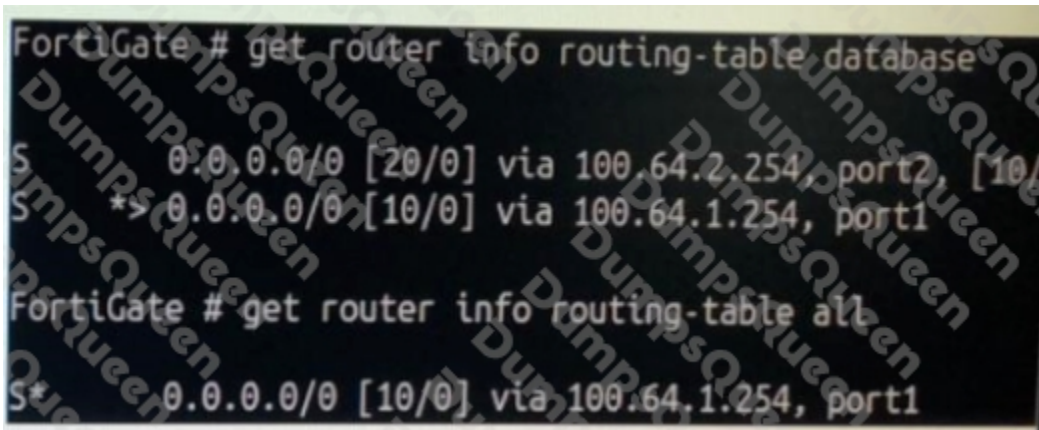
Which two statements about conserve mode are true? (Choose two.)

- A. FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.
- B. FortiGate starts dropping all new sessions when the system memory reaches the configured red threshold.
- C. FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.
- D. FortiGate exits conserve mode when the system memory goes below the configured green threshold.

ANSWER: A D

QUESTION NO: 4

Refer to the exhibit, which contains partial outputs from two routing debug commands.



```
FortiGate # get router info routing-table database
0.0.0.0/0 [20/0] via 100.64.2.254, port2 [10/0]
* 0.0.0.0/0 [10/0] via 100.64.1.254, port1

FortiGate # get router info routing-table all
0.0.0.0/0 [10/0] via 100.64.1.254, port1
```

Why is the port2 default route not in the second command's output?

- A. It has a higher priority value than the default route using port1.
- B. It is disabled in the FortiGate configuration.
- C. It has a lower priority value than the default route using port1.

D. It has a higher distance than the default route using port1.

ANSWER: D

QUESTION NO: 5

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.

ANSWER: B

QUESTION NO: 6

Refer to the exhibit, which contains the partial output of the get vpn ipsec tunnel details command.

```
Hub # get vpn ipsec tunnel details
gateway
  name: 'Hub2Spokel'
  type: route-based
  local-gateway: 10.10.1.1:0 (static)
  remote-gateway: 10.10.2.2:0 (static)
  mode: ike-v1
  interface: 'wan2' (6)
  rx packets: 1025 bytes: 524402 errors: 0
  tx packets: 641 bytes: 93 errors: 0
  dpd: on-demand/negotiated idle: 20000ms retry: 3 count: 0
  selectors
    name: 'Hub2Spokel'
    auto-negotiate: disable
    mode: tunnel
    src: 0:192.168.1.0/0.0.0.0:0
    dst: 0:10.10.20.0/0.0.0.0:0
  SA
    lifetime/rekey: 43200/32137
    mtu: 1438
    tx-esp-seq: 2ce
    replay: enabled
    inbound
      spi: 01e54b14
      enc: aes-cb 914dc5d092667ed436ea7f6efb867976
      auth: sha1 a81b019d4cdfda32ce51e6b01d0b1ea42a74adce
    outbound
      spi: 3dd3545f
      enc: aes-cb 017b8ff6c4ba21eac99b22380b7de74d
      auth: sha1 edd8141f4956140eef703d9042621d3dbf5cd961
  NPU acceleration: encryption(outbound) decryption(inbound)
```

Based on the output, which two statements are correct? (Choose two.)

- A. The npu_flag for this tunnel is 03.
- B. Different SPI values are a result of auto-negotiation being disabled for phase 2 selectors.
- C. Anti-replay is enabled.
- D. The npu_flag for this tunnel is 02.

ANSWER: A C

QUESTION NO: 7

Examine the output of the 'get router info ospf interface' command shown in the exhibit; 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 statements are true regarding the above output? (Choose two.)

- A. The port4 interface is connected to the OSPF backbone area.
- B. The local FortiGate has been elected as the OSPF backup designated router.
- C. There are at least 5 OSPF routers connected to the port4 network.
- D. Two OSPF routers are down in the port4 network.

ANSWER: A C

Explanation:

on BROADCAST network there are 4 neighbors, among which 1*DR +1*BDR. So our FG has 4 neighbors, but create adjacency only with 2 (with DR and BDR). 2 neighbors DROther (not down).

QUESTION NO: 8

Refer to the exhibit, which shows a partial web filter profile configuration.

FortiGuard Category Based Filter

Name	Action
<input type="checkbox"/> Bandwidth Consuming 6	
Freeware and Software Downloads	<input checked="" type="checkbox"/> Allow
File Sharing and Storage	<input type="checkbox"/> Block

Static URL Filter

URL Filter

URL	Type	Action	Status
*.dropbox.com	Wildcard	<input checked="" type="checkbox"/> Allow	<input checked="" type="checkbox"/> Enable

Content Filter

Pattern Type	Pattern	Language	Action	Status
Wildcard	*dropbox*	Western	<input type="checkbox"/> Exempt	<input checked="" type="checkbox"/> Enable

Which action will FortiGate take if a user attempts to access www.dropbox.com, which is categorized as File Sharing and Storage?

- A. FortiGate will block the connection, based on the FortiGuard category based filter configuration.
- B. FortiGate will block the connection as an invalid URL.
- C. FortiGate will exempt the connection, based on the Web Content Filter configuration.
- D. FortiGate will allow the connection, based on the URL Filter configuration.

ANSWER: A

Explanation:

Enterprise_Firewall_7.0_Study_Guide-Online.pdf p 351 url filter -> FortiGuard Web Filter -> Web Content Filter -> Advanced Filter Options Allow -> Block

QUESTION NO: 9

An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device.

What can the administrator do to fix this problem?

- A. Configure remote link monitoring to detect an issue in the forwarding path.
- B. Configure set send-garp-on-failover enable under config system ha on both cluster members.
- C. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports.
- D. Configure set link-failed-signal enable under config system ha on both cluster members.

ANSWER: D

Explanation:

Virtual MAC Address and Failover - The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port. - Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces): #Config system ha set link-failed-signal enable end - This simulates a link failure that clears the related entries from MAC table of the switches.

QUESTION NO: 10

Refer to the exhibit, which contains the output of the diagnose vpn tunnel list.

Which command will capture ESP traffic for the VPN named DialUp_0?

- A. diagnose sniffer packet any 'esp and host 10.200.3.2'
- B. diagnose sniffer packet any 'ip proto 50'
- C. diagnose sniffer packet any 'host 10.0.10.10'
- D. diagnose sniffer packet any 'port 4500'

ANSWER: D