Free Questions for NSE7_SDW-7.2 by go4braindumps

Shared by Tucker on 22-07-2024

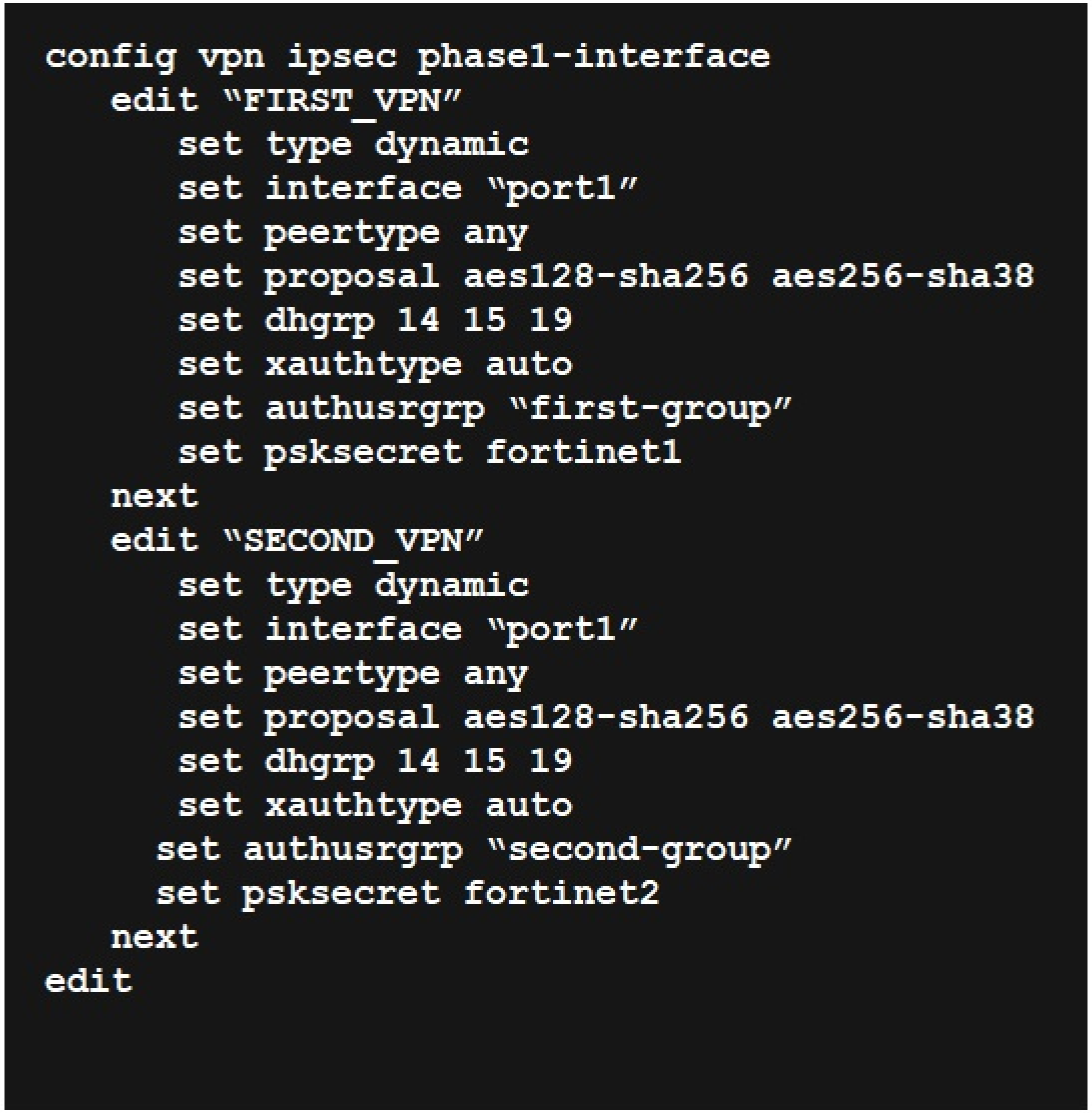
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Refer to the exhibit.



```
config vpn ipsec phase1-interface
   edit “FIRST_VPN”
      set type dynamic
      set interface “port1”
      set peertype any
      set proposal aes128-sha256 aes256-sha38
      set dhgrp 14 15 19
      set xauthtype auto
      set authusrgrp “first-group”
      set psksecret fortinet1
   next
   edit “SECOND_VPN”
      set type dynamic
      set interface “port1”
      set peertype any
      set proposal aes128-sha256 aes256-sha38
      set dhgrp 14 15 19
      set xauthtype auto
     set authusrgrp “second-group”
     set psksecret fortinet2
   next
edit
```

FortiGate has multiple dial-up VPN interfaces incoming on port1 that match only FIRST_VPN.

Which two configuration changes must be made to both IPsec VPN interfaces to allow incoming connections to match all possible IPsec dial-up interfaces? (Choose two.)

Options:

A- Specify a unique peer ID for each dial-up VPN interface.

B- Use different proposals are used between the interfaces.

C- Configure the IKE mode to be aggressive mode.

D- Use unique Diffie Hellman groups on each VPN interface.

Answer:

A, C

Question 2

Question Type: **MultipleChoice**

In the default SD-WAN minimum configuration, which two statements are correct when traffic matches the default implicit SD-WAN rule? (Choose two)

Options:

A- Traffic has matched none of the FortiGate policy routes.

B- Matched traffic failed RPF and was caught by the rule.

C- The FIB lookup resolved interface was the SD-WAN interface.

D- An absolute SD-WAN rule was defined and matched traffic.

Answer:

A, C

Question 3

Question Type: MultipleChoice

What are two reasons for using FortiManager to organize and manage the network for a group of FortiGate devices? (Choose two.)

Options:

A- It simplifies the deployment and administration of SD-WAN on managed FortiGate devices.

B- It improves SD-WAN performance on the managed FortiGate devices.

C- It sends probe signals as health checks to the beacon servers on behalf of FortiGate.

D- It acts as a policy compliance entity to review all managed FortiGate devices.

E- It reduces WAN usage on FortiGate devices by acting as a local FortiGuard server.

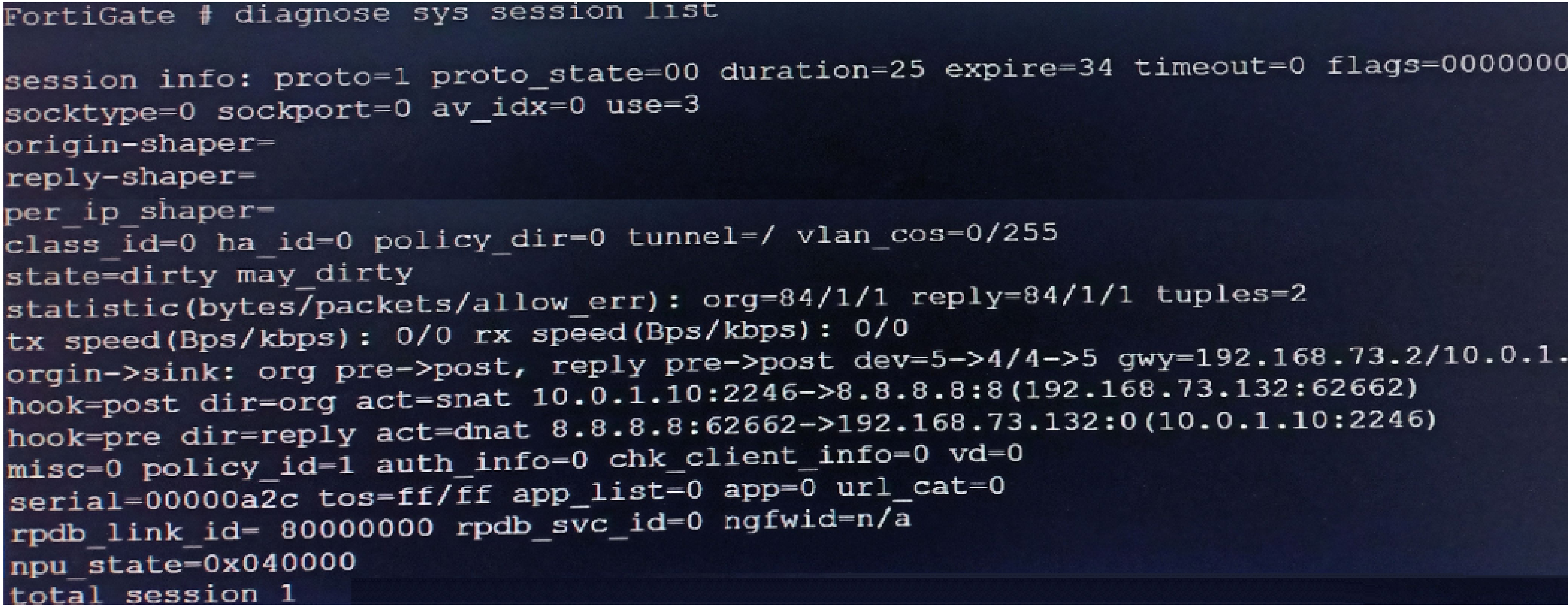
Answer:

A, E

Question 4

Question Type: **MultipleChoice**

Refer to the exhibit.



```
FortiGate # diagnose sys session list

session info: proto=1 proto_state=00 duration=25 expire=34 timeout=0 flags=0000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=dirty may_dirty
statistic(bytes/packets/allow_err): org=84/1/1 reply=84/1/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=5->4/4->5 gwy=192.168.73.2/10.0.1.
hook=post dir=org act=snat 10.0.1.10:2246->8.8.8.8:8(192.168.73.132:62662)
hook=pre dir=reply act=dnat 8.8.8.8:62662->192.168.73.132:0(10.0.1.10:2246)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000a2c tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 80000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
total session 1
```

Based on the exhibit, which statement about FortiGate re-evaluating traffic is true?

Options:

A- The type of traffic defined and allowed on firewall policy ID 1 is UDP.

B- FortiGate has terminated the session after a change on policy ID 1.

C- Changes have been made on firewall policy ID 1 on FortiGate.

D- Firewall policy ID 1 has source NAT disabled.

Answer:

C

Question 5

Question Type: **MultipleChoice**

Which two statements describe how IPsec phase 1 main mode is different from aggressive mode when performing IKE negotiation? (Choose two)

Options:

A- A peer ID is included in the first packet from the initiator, along with suggested security policies.

B- XAuth is enabled as an additional level of authentication, which requires a username and password.

C- A total of six packets are exchanged between an initiator and a responder instead of three packets.

D- The use of Diffie Hellman keys is limited by the responder and needs initiator acceptance.

Answer:

B, C

Question 6

Question Type: MultipleChoice

What are two reasons why FortiGate would be unable to complete the zero-touch provisioning process? (Choose two.)

Options:

A- The FortiGate cloud key has not been added to the FortiGate cloud portal.

B- FortiDeploy has connected with FortiGate and provided the initial configuration to contact FortiManager

C- The zero-touch provisioning process has completed internally, behind FortiGate.

D- FortiGate has obtained a configuration from the platform template in FortiGate cloud.

E- A factory reset performed on FortiGate.

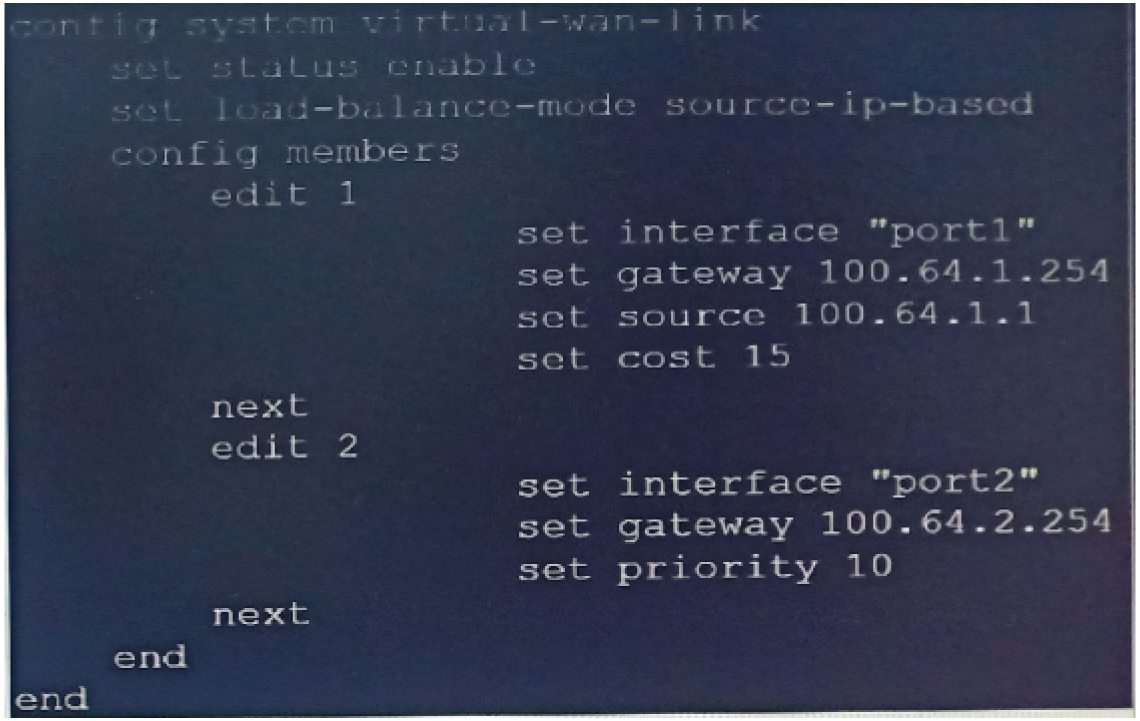
Answer:

A, C

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



```
config system virtual-wan-link
    set status enable
    set load-balance-mode source-ip-based
    config members
        edit 1
                    set interface "port1"
                    set gateway 100.64.1.254
                    set source 100.64.1.1
                    set cost 15
        next
        edit 2
                    set interface "port2"
                    set gateway 100.64.2.254
                    set priority 10
        next
    end
end
```

Based on the output shown in the exhibit, which two criteria on the SD-WAN member configuration can be used to select an outgoing interface in an SD-WAN rule? (Choose two.)

Options:

A- Set priority 10.

B- Set cost 15.

C- Set load-balance-mode source-ip-ip-based.

D- Set source 100.64.1.1.

Answer:

A, B

Question 8

Question Type: **MultipleChoice**

Which components make up the secure SD-WAN solution?

Options:

A- Application, antivirus, and URL, and SSL inspection

B- Datacenter, branch offices, and public cloud

C- FortiGate, FortiManager, FortiAnalyzer, and FortiDeploy

D- Telephone, ISDN, and telecom network.

Answer:

C

Question 9

Question Type: **MultipleChoice**

In a hub-and-spoke topology, what are two advantages of enabling ADVPN on the IPsec overlays? (Choose two.)

Options:

A- It provides the benefits of a full-mesh topology in a hub-and-spoke network.

B- It provides direct connectivity between spokes by creating shortcuts.

C- It enables spokes to bypass the hub during shortcut negotiation.

D- It enables spokes to establish shortcuts to third-party gateways.

Answer:

A, B

Question 10

Question Type: MultipleChoice

Which best describes the SD-WAN traffic shaping mode that bases itself on a percentage of available bandwidth?

Options:

A- Interface-based shaping mode

B- Reverse-policy shaping mode

C- Shared-policy shaping mode

D- Per-IP shaping mode

Answer:

A

Explanation:

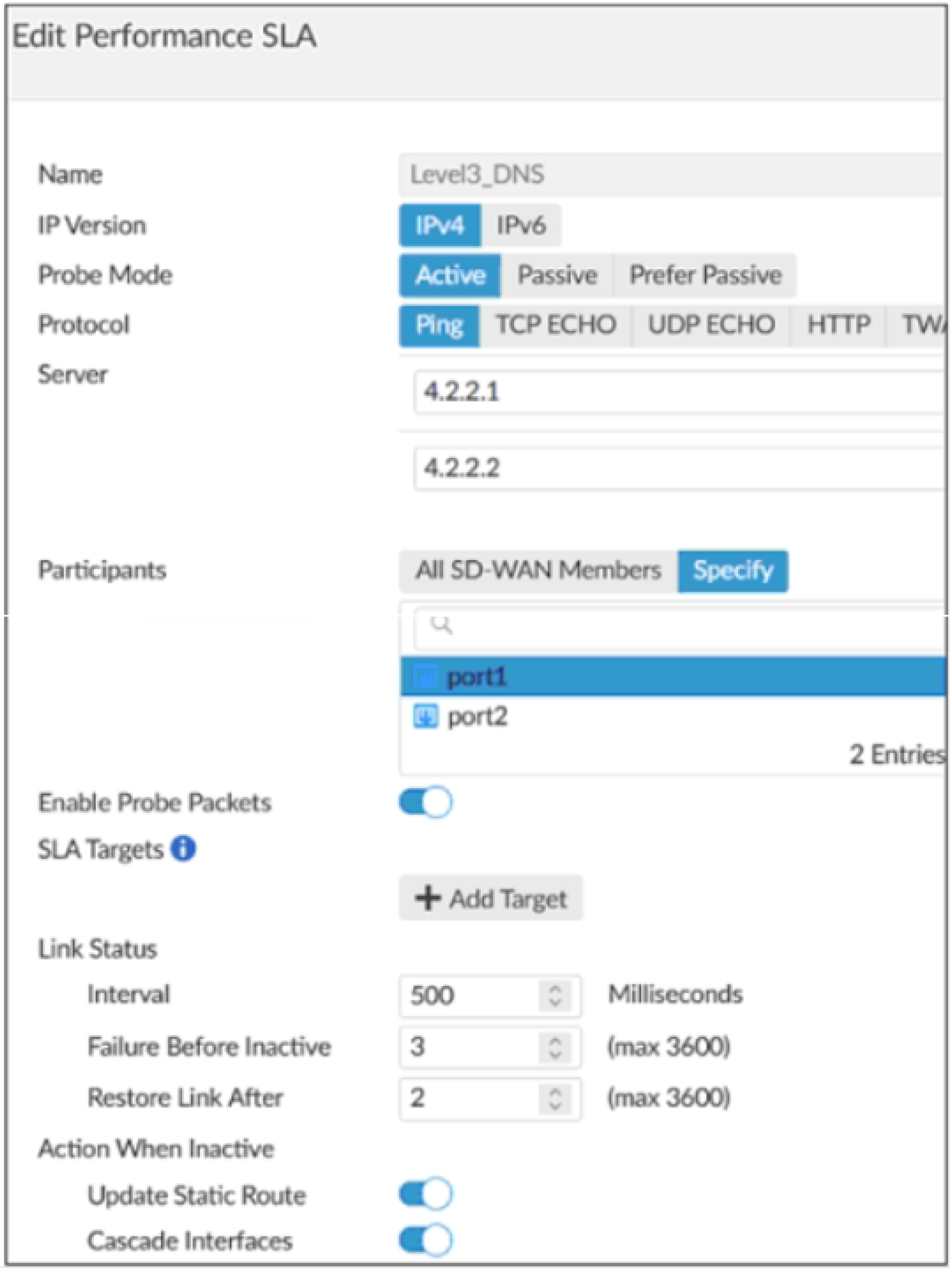
Interface-based shaping goes further, enabling traffic controls based on percentage of the interface bandwidth.

Question 11

Question Type: MultipleChoice

Refer to the exhibits.

Exhibit A -



Edit Performance SLA

Name: Level3_DNS

IP Version: [✓ IPv4] IPv6

Probe Mode: [✓ Active] Passive Prefer Passive

Protocol: [✓ Ping] TCP ECHO UDP ECHO HTTP TW

Server: 4.2.2.1

4.2.2.2

Participants: All SD-WAN Members [✓ Specify]

- port1
- port2

2 Entries

Enable Probe Packets: ●

SLA Targets

Link Status

Interval: 500 Milliseconds

Failure Before Inactive: 3 (max 3600)

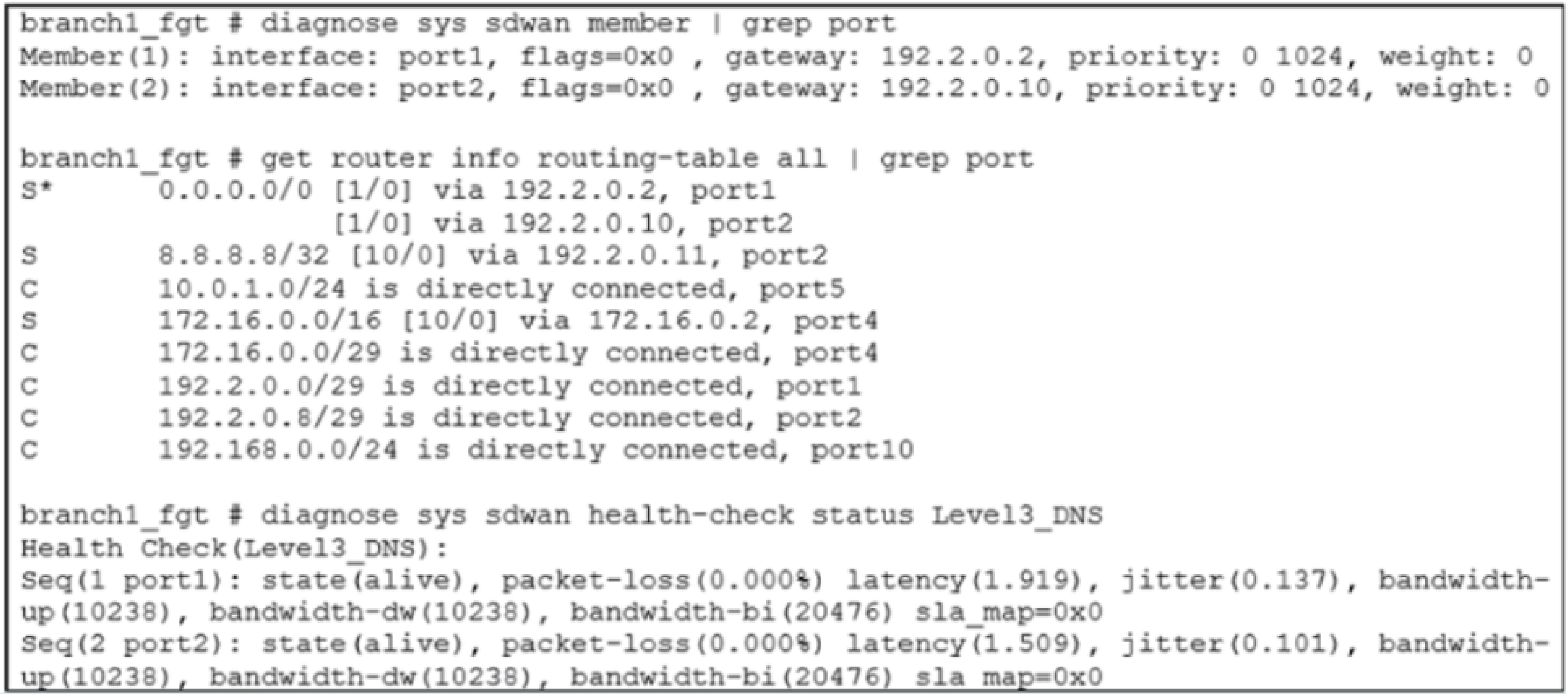
Restore Link After: 2 (max 3600)

Action When Inactive

Update Static Route: ●

Cascade Interfaces: ●

Exhibit B -



```
branch1_fgt # diagnose sys sdwan member | grep port
Member(1): interface: port1, flags=0x0 , gateway: 192.2.0.2, priority: 0 1024, weight: 0
Member(2): interface: port2, flags=0x0 , gateway: 192.2.0.10, priority: 0 1024, weight: 0

branch1_fgt # get router info routing-table all | grep port
S*       0.0.0.0/0 [1/0] via 192.2.0.2, port1
                   [1/0] via 192.2.0.10, port2
S        8.8.8.8/32 [10/0] via 192.2.0.11, port2
C        10.0.1.0/24 is directly connected, port5
S        172.16.0.0/16 [10/0] via 172.16.0.2, port4
C        172.16.0.0/29 is directly connected, port4
C        192.2.0.0/29 is directly connected, port1
C        192.2.0.8/29 is directly connected, port2
C        192.168.0.0/24 is directly connected, port10

branch1_fgt # diagnose sys sdwan health-check status Level3_DNS
Health Check(Level3_DNS):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(1.919), jitter(0.137), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(1.509), jitter(0.101), bandwidth-
up(10238), bandwidth-dw(10238), bandwidth-bi(20476) sla_map=0x0
```

Exhibit A shows the SD-WAN performance SLA and exhibit B shows the SD-WAN member status, the routing table, and the performance SLA status.

If port2 is detected dead by FortiGate, what is the expected behavior?

Options:

A- Port2 becomes alive after three successful probes are detected.

B- FortiGate removes all static routes for port2.

C- The administrator manually restores the static routes for port2, if port2 becomes alive.

D- Host 8.8.8.8 is reachable through port1 and port2.

Answer:

B

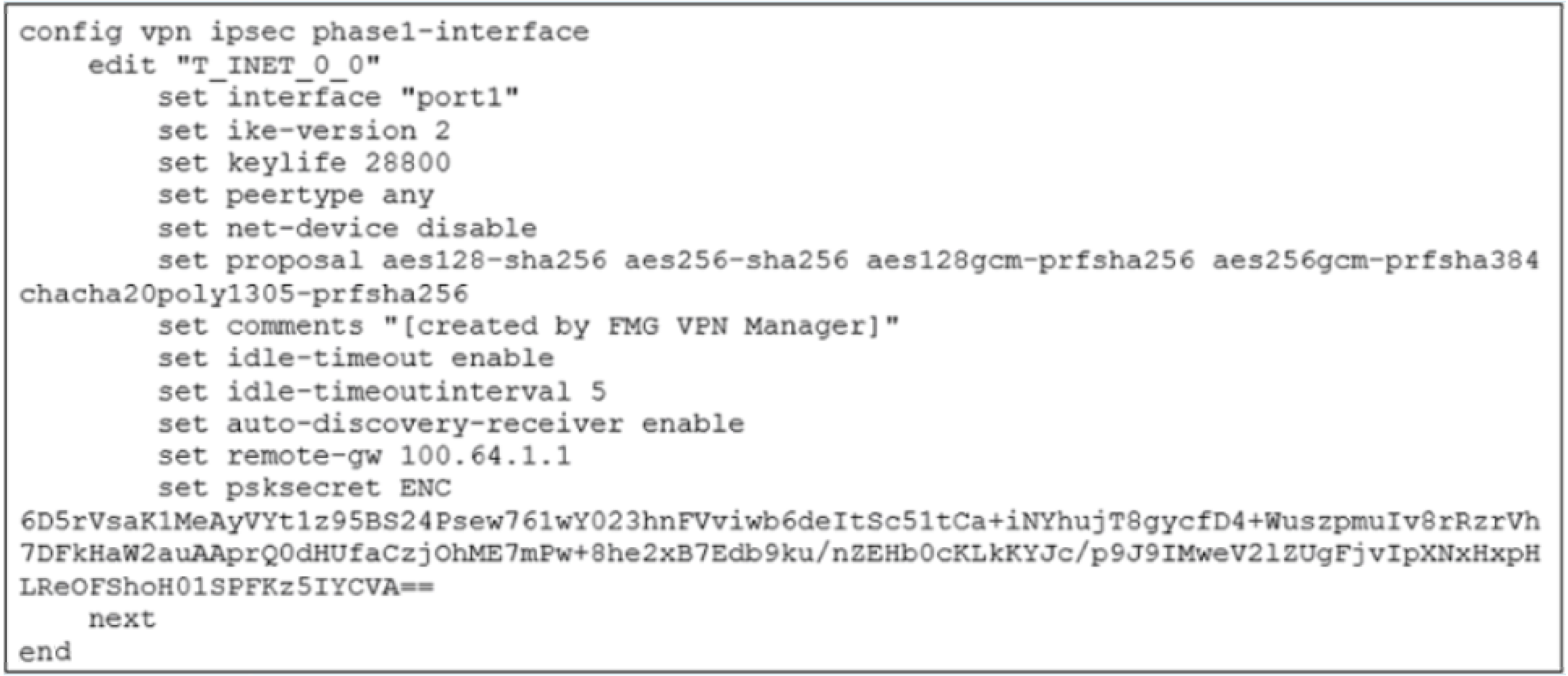
Explanation:

This is due to Update static route is enable which removes the static route entry referencing the interface if the interface is dead

Question 12

Question Type: MultipleChoice

Refer to the exhibit, which shows the IPsec phase 1 configuration of a spoke.



```
config vpn ipsec phase1-interface
    edit "T_INET_0_0"
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384
chacha20poly1305-prfsha256
        set comments "[created by FMG VPN Manager]"
        set idle-timeout enable
        set idle-timeoutinterval 5
        set auto-discovery-receiver enable
        set remote-gw 100.64.1.1
        set psksecret ENC
6D5rVsaK1MeAyVYt1z95BS24Psew761wY023hnFVviwb6deItSc51tCa+iNYhujT8gycfD4+WuszpmuIv8rRzrVh
7DFkHaW2auAAprQ0dHUfaCzjOhME7mPw+8he2xB7Edb9ku/nZEHb0cKLkKYJc/p9J9IMweV2lZUgFjvIpXNxHxpH
LReOFShoH01SPFKz5IYCVA==
    next
end
```

What must you configure on the IPsec phase 1 configuration for ADVPN to work with SD-WAN?

Options:

A- You must set ike-version to 1.

B- You must enable net-device.

C- You must enable auto-discovery-sender.

D- You must disable idle-timeout.

Answer:

B