Free Questions for NSE8_812 by vceexamstest

Shared by Kelly on 19-06-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You must configure an environment with dual-homed servers connected to a pair of FortiSwitch units using an MCLAG.

Multicast traffic is expected in this environment, and you should ensure unnecessary traffic is pruned from links that do not have a multicast listener.

In which two ways must you configure the igmps-f lood-traffic and igmps-flood-report settings? (Choose two.)

Options:

A- disable on ICL trunks

B- enable on ICL trunks

C- disable on the ISL and FortiLink trunks

D- enable on the ISL and FortiLink trunks

Answer:

A, C

Explanation:

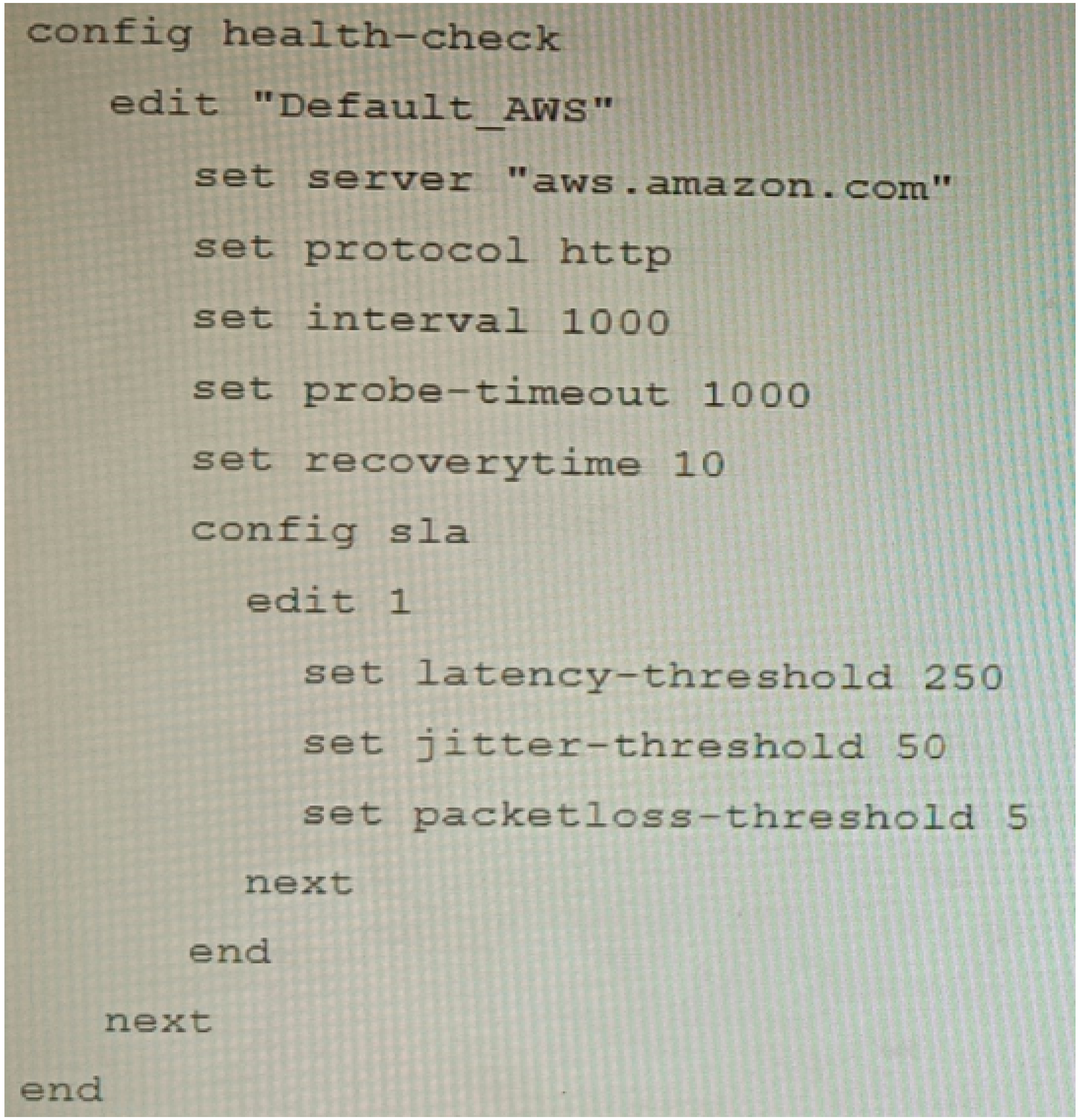
A is correct because disabling igmps-flood-traffic and igmps-flood-report on ICL trunks prevents unnecessary multicast traffic from being flooded across the MCLAG cluster members. C is correct because disabling igmps-flood-traffic and igmps-flood-report on the ISL and FortiLink trunks prevents unnecessary multicast traffic from being flooded to other switches or FortiGates that do not have multicast listeners. Reference: https://docs.fortinet.com/document/fortiswitches/6.4.0/administration-guide/381057/multicast-forwarding https://docs.fortinet.com/document/fortiswitches/6.4.0/administration-guide/381057/multicast-forwarding/381058/configuring-multicast-forwarding

Question 2

Question Type: MultipleChoice

You are creating the CLI script to be used on a new SD-WAN deployment You will have branches with a different number of internet connections and want to be sure there is no need to change the Performance SLA configuration in case more connections are added to the branch.

The current configuration is:



```
config health-check
   edit "Default_AWS"
      set server "aws.amazon.com"
      set protocol http
      set interval 1000
      set probe-timeout 1000
      set recoverytime 10
      config sla
        edit 1
          set latency-threshold 250
          set jitter-threshold 50
          set packetloss-threshold 5
        next
      end
   next
end
```

Which configuration do you use for the Performance SLA members?

Options:

A- set members any

B- set members 0

C- current configuration already fulfills the requirement

D- set members all

Answer:

D

Explanation:

D is correct because using set members all allows you to apply the Performance SLA configuration to all available interfaces without specifying them individually. This way, you do not need to change the configuration in case more connections are added to the branch.

Reference: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/sd-wan

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/sd-wan/978795/configuring-sd-wan-performance-sla

Question 3

Question Type: MultipleChoice

Refer to the exhibits.

The exhibits show a diagram of a requested topology and the base IPsec configuration.

A customer asks you to configure ADVPN via two internet underlays. The requirement is that you use one interface with a single IP address on DC FortiGate.

In this scenario, which feature should be implemented to achieve this requirement?

Options:

A- Use network-overlay id

B- Change advpn2 to IKEv1

C- Use local-id

D- Use peer-id

Answer:

A

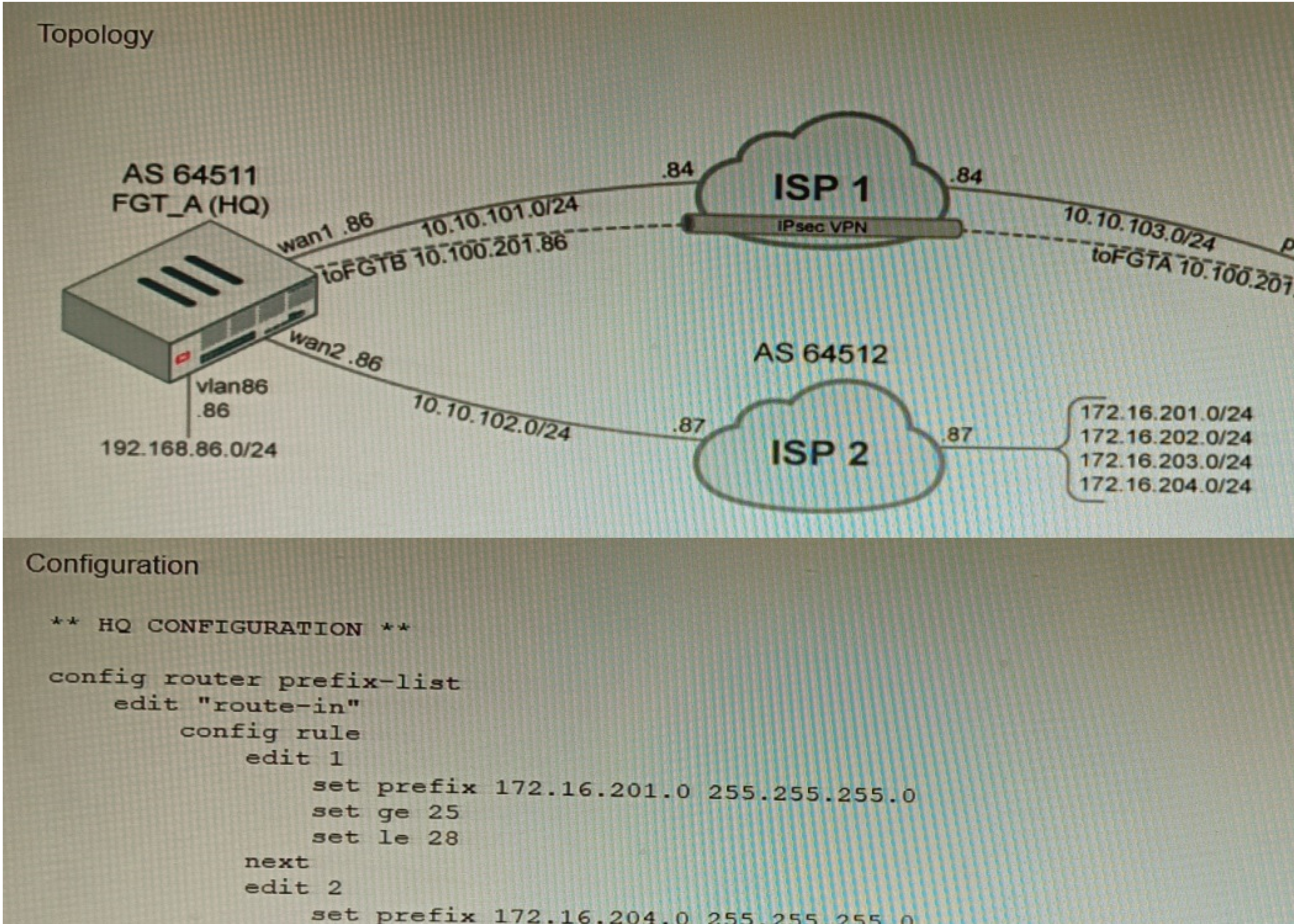
Explanation:

A is correct because using network-overlay id allows you to configure multiple ADVPN tunnels on a single interface with a single IP address on the DC FortiGate. This is explained in the FortiGate Administration Guide under ADVPN > Configuring ADVPN > Configuring ADVPN on the hub. Reference: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn/978794/configuring-advpn

Question 4

Question Type: MultipleChoice

Refer to the exhibits.



Topology

Configuration

```
** HQ CONFIGURATION **

config router prefix-list
    edit "route-in"
        config rule
            edit 1
                set prefix 172.16.201.0 255.255.255.0
                set ge 25
                set le 28
            next
            edit 2
                set prefix 172.16.204.0 255.255.255.0
```

A customer has deployed a FortiGate with iBGP and eBGP routing enabled. HQ is receiving routes over eBGP from ISP 2; however, only certain routes are showing up in the routing table-Assume that BGP is working perfectly and that the only possible modifications to the routing table are solely due to the prefix list that is applied on HQ.

Given the exhibits, which two routes will be active in the routing table on the HQ firewall? (Choose two.)

Options:

A- 172.16.204.128/25

B- 172.16.201.96/29

C- 172,620,64,27

D- 172.16.204.64/27

Answer:

A, C

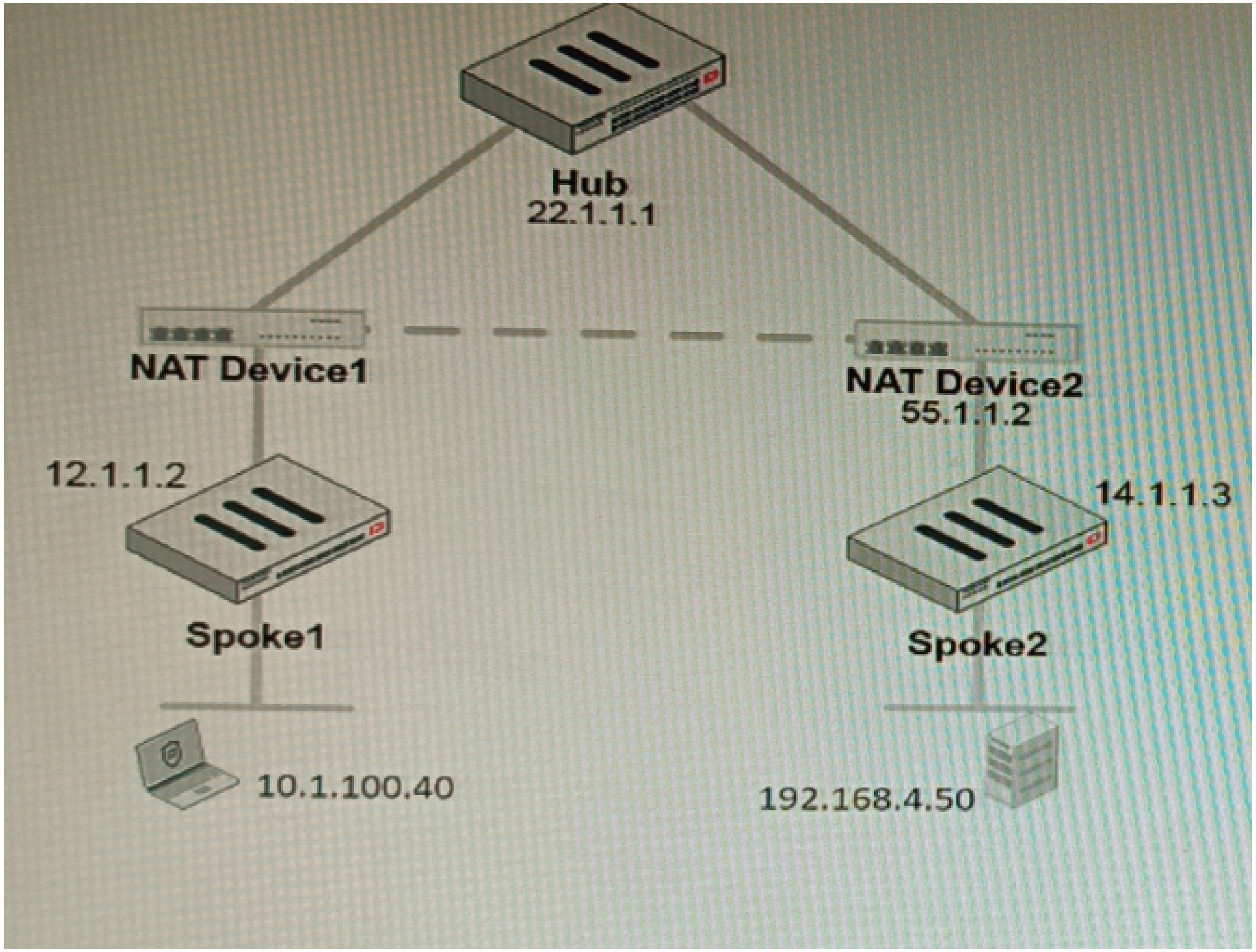
Explanation:

A is correct because 172.16.204.128/25 matches the prefix list entry 172.16.204.0/24 ge 25 le 25. C is correct because 172.16.204.64/27 matches the prefix list entry 172.16.204.0/24 ge 27 le 27. Reference: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/bgp

Question 5

Question Type: **MultipleChoice**

Refer to the exhibit, which shows a VPN topology.



The device IP 10.1.100.40 downloads a file from the FTP server IP 192.168.4.50

Referring to the exhibit, what will be the traffic flow behavior if ADVPN is configured in this environment?

Options:

A- All the session traffic will pass through the Hub

B- The TCP port 21 must be allowed on the NAT Device2

C- ADVPN is not supported when spokes are behind NAT

D- Spoke1 will establish an ADVPN shortcut to Spoke2

Answer:

D

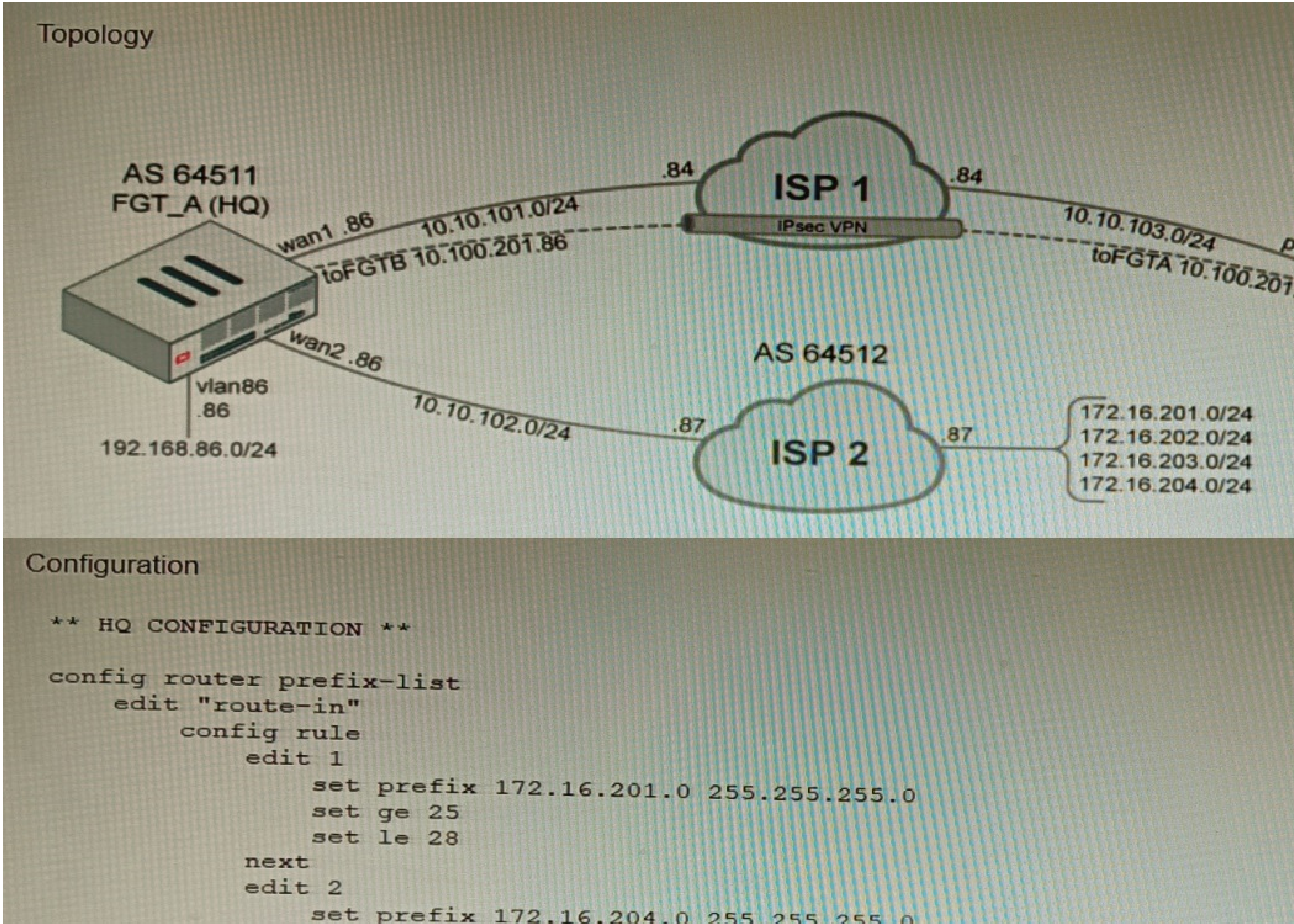
Explanation:

D is correct because Spoke1 will establish an ADVPN shortcut to Spoke2 when it detects that there is a demand for traffic between them. This is explained in the Fortinet Community article on Technical Tip: Fortinet Auto Discovery VPN (ADVPN) under Summary - ADVPN sequence of events. Reference: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Fortinet-Auto-Discovery-VPN-ADVPN/ta-p/195698

Question 6

Question Type: **MultipleChoice**

Refer to the exhibits.



Topology

Configuration

```
 ** HQ CONFIGURATION **

config router prefix-list
    edit "route-in"
        config rule
            edit 1
                set prefix 172.16.201.0 255.255.255.0
                set ge 25
                set le 28
            next
            edit 2
                set prefix 172.16.204.0 255.255.255.0
```

A customer has deployed a FortiGate with iBGP and eBGP routing enabled. HQ is receiving routes over eBGP from ISP 2; however, only certain routes are showing up in the routing table-Assume that BGP is working perfectly and that the only possible modifications to the routing table are solely due to the prefix list that is applied on HQ.

Given the exhibits, which two routes will be active in the routing table on the HQ firewall? (Choose two.)

Options:

A- 172.16.204.128/25

B- 172.16.201.96/29

C- 172,620,64,27

D- 172.16.204.64/27

Answer:

A, C

Explanation:

A is correct because 172.16.204.128/25 matches the prefix list entry 172.16.204.0/24 ge 25 le 25. C is correct because 172.16.204.64/27 matches the prefix list entry 172.16.204.0/24 ge 27 le 27. Reference: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/bgp

Question 7

Question Type: **MultipleChoice**

You must configure an environment with dual-homed servers connected to a pair of FortiSwitch units using an MCLAG.

Multicast traffic is expected in this environment, and you should ensure unnecessary traffic is pruned from links that do not have a multicast listener.

In which two ways must you configure the igmps-f lood-traffic and igmps-flood-report settings? (Choose two.)

Options:

A- disable on ICL trunks

B- enable on ICL trunks

C- disable on the ISL and FortiLink trunks

D- enable on the ISL and FortiLink trunks

Answer:

A, C

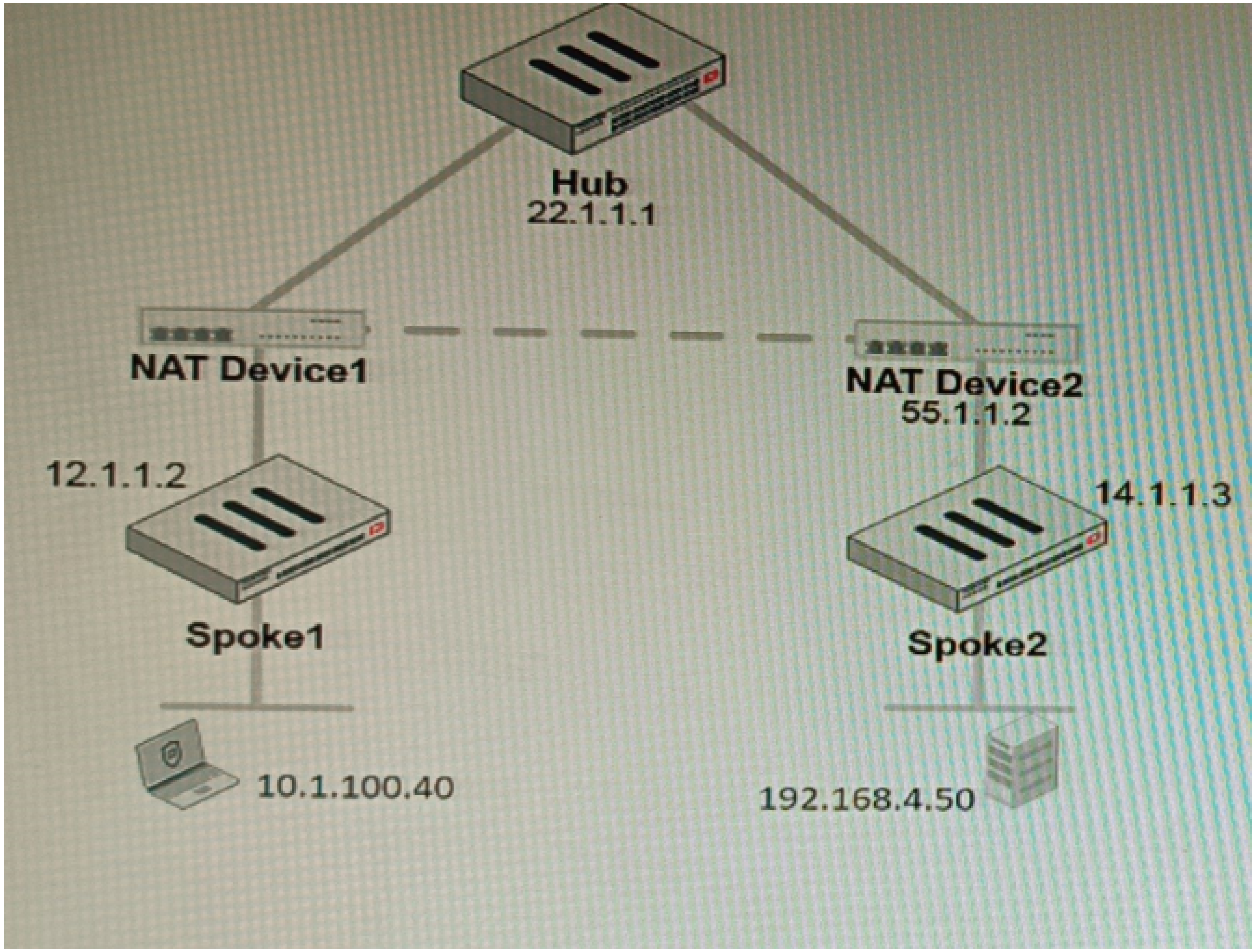
Explanation:

A is correct because disabling igmps-flood-traffic and igmps-flood-report on ICL trunks prevents unnecessary multicast traffic from being flooded across the MCLAG cluster members. C is correct because disabling igmps-flood-traffic and igmps-flood-report on the ISL and FortiLink trunks prevents unnecessary multicast traffic from being flooded to other switches or FortiGates that do not have multicast listeners. Reference: https://docs.fortinet.com/document/fortiswitches/6.4.0/administration-guide/381057/multicast-forwarding https://docs.fortinet.com/document/fortiswitches/6.4.0/administration-guide/381057/multicast-forwarding/381058/configuring-multicast-forwarding

Question 8

Question Type: MultipleChoice

Refer to the exhibit, which shows a VPN topology.



The device IP 10.1.100.40 downloads a file from the FTP server IP 192.168.4.50

Referring to the exhibit, what will be the traffic flow behavior if ADVPN is configured in this environment?

Options:

A- All the session traffic will pass through the Hub

B- The TCP port 21 must be allowed on the NAT Device2

C- ADVPN is not supported when spokes are behind NAT

D- Spoke1 will establish an ADVPN shortcut to Spoke2

Answer:

D

Explanation:

D is correct because Spoke1 will establish an ADVPN shortcut to Spoke2 when it detects that there is a demand for traffic between them. This is explained in the Fortinet Community article on Technical Tip: Fortinet Auto Discovery VPN (ADVPN) under Summary - ADVPN sequence of events. Reference: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Fortinet-Auto-Discovery-VPN-ADVPN/ta-p/195698

Question 9

Question Type: **MultipleChoice**

Refer to the exhibits.

The exhibits show a diagram of a requested topology and the base IPsec configuration.

A customer asks you to configure ADVPN via two internet underlays. The requirement is that you use one interface with a single IP address on DC FortiGate.

In this scenario, which feature should be implemented to achieve this requirement?

Options:

A- Use network-overlay id

B- Change advpn2 to IKEv1

C- Use local-id

D- Use peer-id

Answer:

A

Explanation:

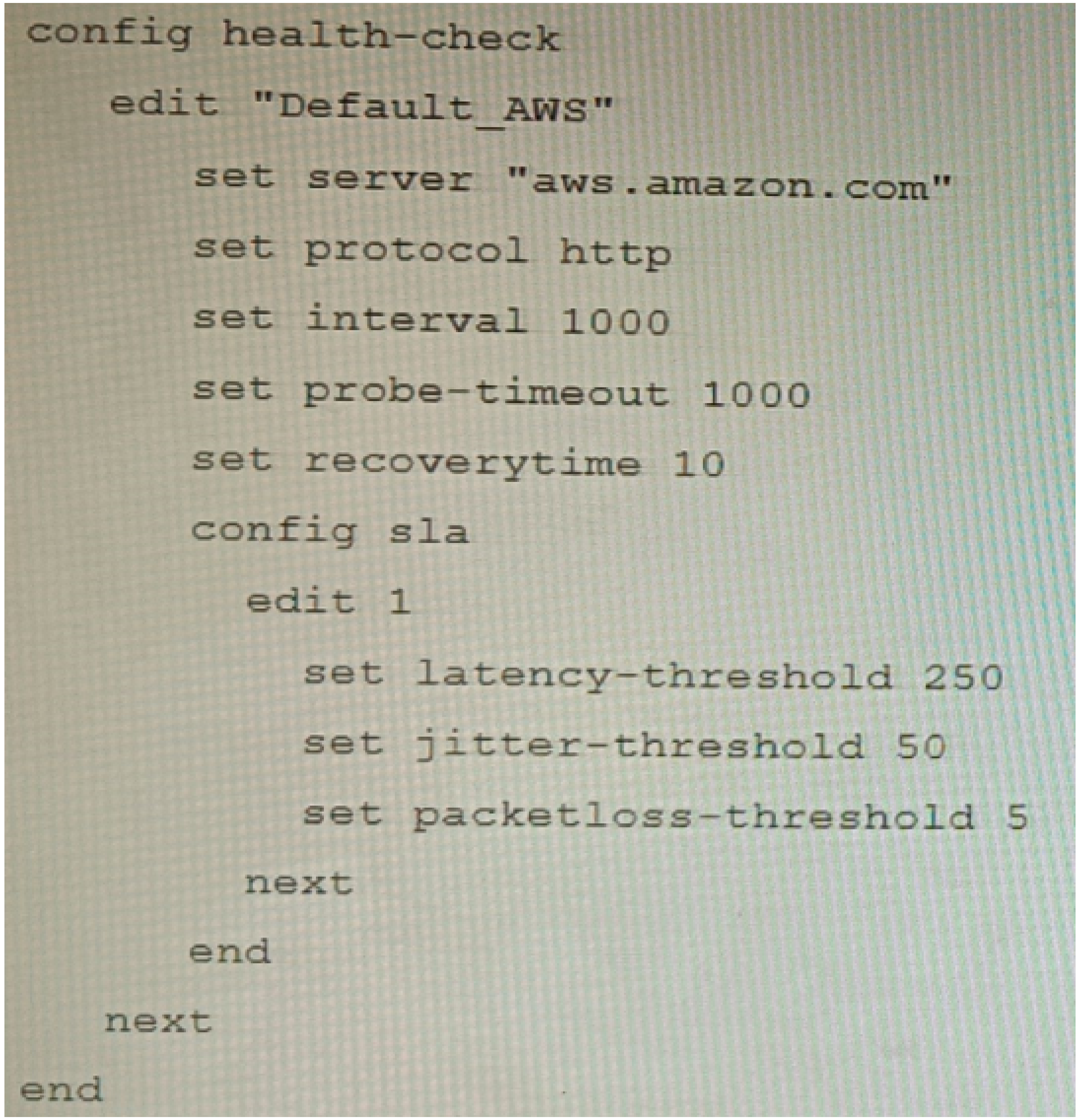
A is correct because using network-overlay id allows you to configure multiple ADVPN tunnels on a single interface with a single IP address on the DC FortiGate. This is explained in the FortiGate Administration Guide under ADVPN > Configuring ADVPN > Configuring ADVPN on the hub. Reference: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn/978794/configuring-advpn

Question 10

Question Type: MultipleChoice

You are creating the CLI script to be used on a new SD-WAN deployment You will have branches with a different number of internet connections and want to be sure there is no need to change the Performance SLA configuration in case more connections are added to the branch.

The current configuration is:



```
config health-check
    edit "Default_AWS"
        set server "aws.amazon.com"
        set protocol http
        set interval 1000
        set probe-timeout 1000
        set recoverytime 10
        config sla
           edit 1
              set latency-threshold 250
              set jitter-threshold 50
              set packetloss-threshold 5
           next
        end
    next
end
```

Which configuration do you use for the Performance SLA members?

Options:

A- set members any

B- set members 0

C- current configuration already fulfills the requirement

D- set members all

Answer:

D

Explanation:

D is correct because using set members all allows you to apply the Performance SLA configuration to all available interfaces without specifying them individually. This way, you do not need to change the configuration in case more connections are added to the branch.

Reference: https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/sd-wan

https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/sd-wan/978795/configuring-sd-wan-performance-sla