Free Questions for NSE8_812 by braindumpscollection

Shared by Sanford on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A customer's cybersecurity department needs to implement security for the traffic between two VPCs in AWS, but these belong to different departments within the company. The company uses a single region for all their VPCs.

Which two actions will achieve this requirement while keeping separate management of each department's VPC? (Choose two.)

Options:

A- Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster.

B- Create an 1AM account for the cybersecurity department to manage both existing VPC, create a FortiGate HA Cluster on each VPC and IPSEC VPN to force traffic between the VPCs through the FortiGate clusters

C- Migrate all the instances to the same VPC and create 1AM accounts for each department, then implement a new subnet for a FortiGate auto-scaling group and use routing tables to force the traffic through the FortiGate cluster.

D- Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPC to force routing through the FortiGate cluster

Answer:

A, D

Explanation:

To implement security for the traffic between two VPCs in AWS, while keeping separate management of each department's VPC, two possible actions are:

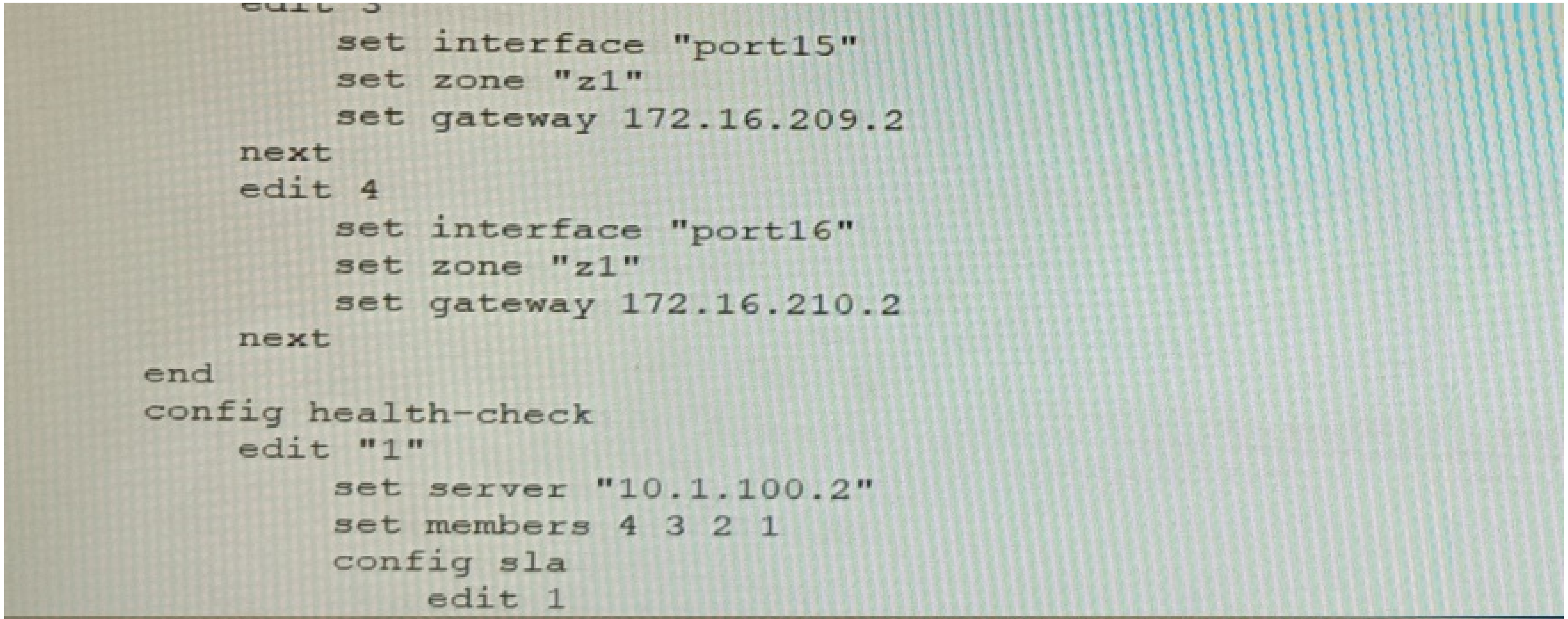
Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster. This option allows the cybersecurity department to manage the transit VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The VPC peering connections enable direct communication between the VPCs without using public IPs or gateways. The routing tables can be configured to direct all inter-VPC traffic to the transit VPC.

Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPCs to force routing through the FortiGate cluster. This option also allows the cybersecurity department to manage the security VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The Transit Gateway acts as a network hub that connects multiple VPCs and on-premises networks. The routing tables can be configured to direct all inter-VPC traffic to the security VPC. References: https://docs.fortinet.com/document/fortigate-public-cloud/7.2.0/aws-administration-guide/506140/connecting-a-local-fortigate-to-an-aws-vpc-vpn https://docs.fortinet.com/document/fortigate-public-cloud/7.0.0/sd-wan-architecture-for-enterprise/166334/sd-wan-configuration

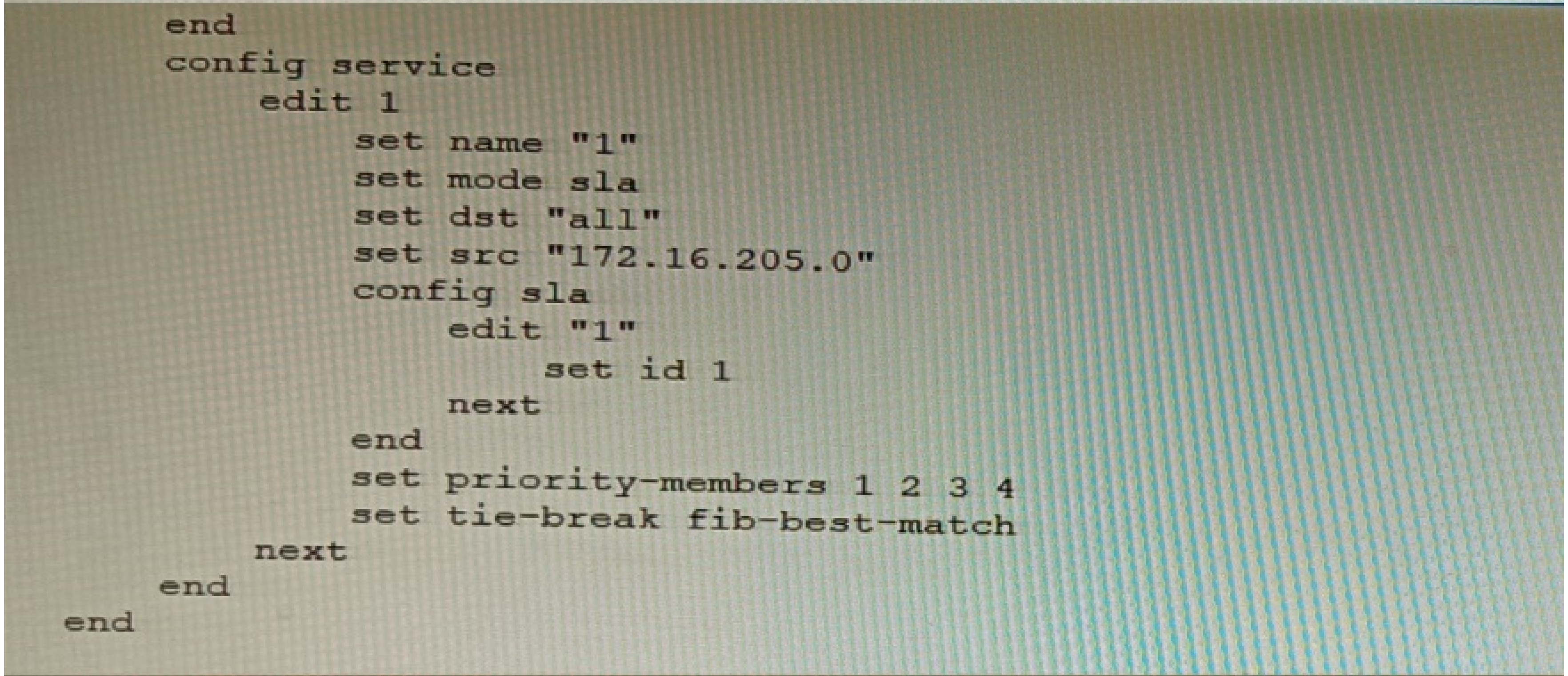
Question 2

Question Type: MultipleChoice

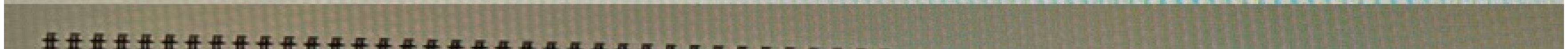
Refer to the exhibit showing an SD-WAN configuration.



```
        edit 3
            set interface "port15"
            set zone "z1"
            set gateway 172.16.209.2
        next
        edit 4
            set interface "port16"
            set zone "z1"
            set gateway 172.16.210.2
        next
    end
    config health-check
        edit "1"
            set server "10.1.100.2"
            set members 4 3 2 1
            config sla
                edit 1
```



```
    end
    config service
        edit 1
            set name "1"
            set mode sla
            set dst "all"
            set src "172.16.205.0"
            config sla
                edit "1"
                    set id 1
                next
            end
            set priority-members 1 2 3 4
            set tie-break fib-best-match
        next
    end
end
```



```
##################################
```

According to the exhibit, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, which outgoing interfaces will be used?

Options:

A- port16 and port1

B- port1 and port1

C- port16 and port15

D- port1 and port15

Answer:

A

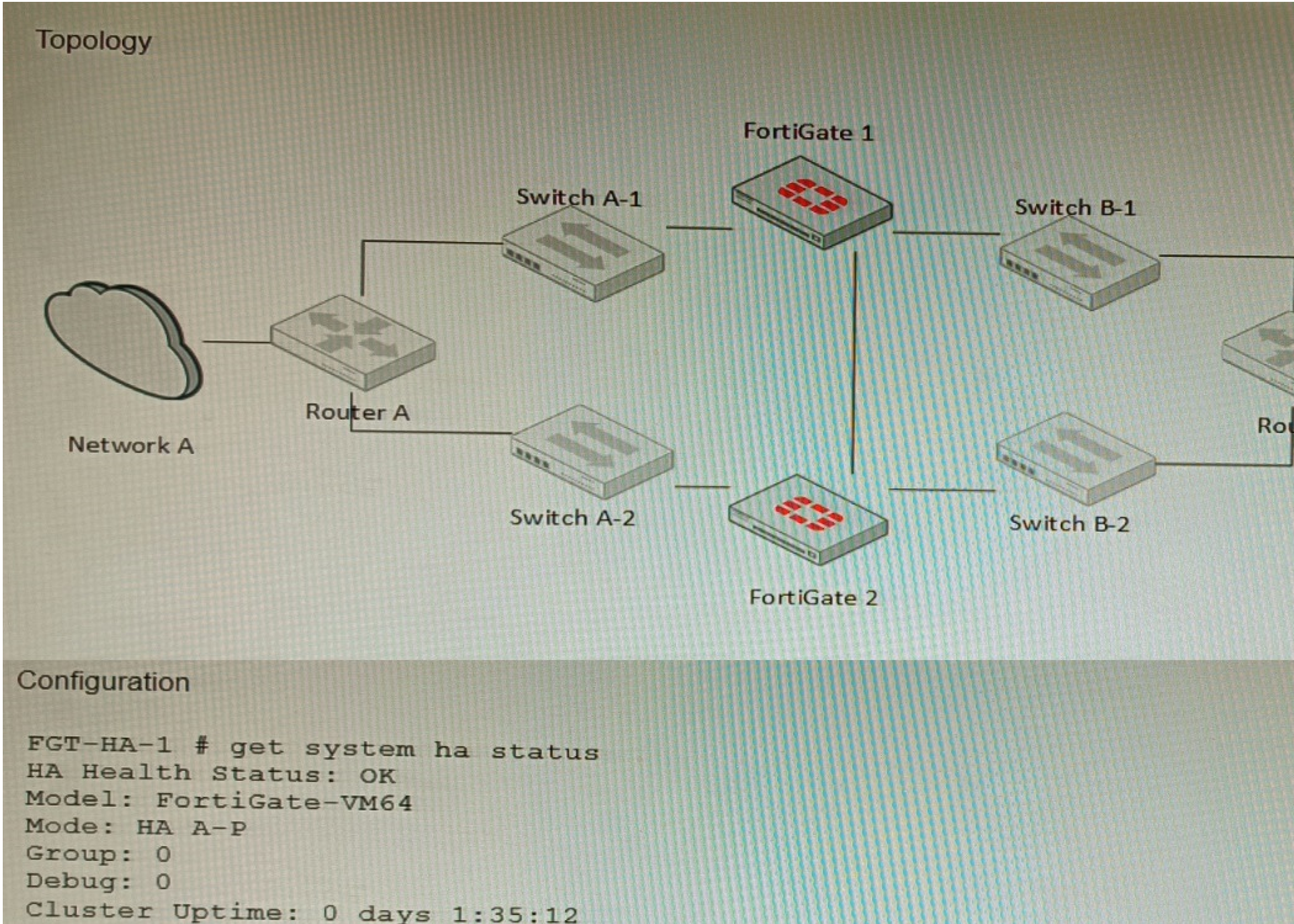
Explanation:

According to the exhibit, the SD-WAN configuration has two rules: one for traffic to 10.1.100.0/24 subnet, and one for traffic to 10.1.100.16/28 subnet. The first rule uses the best quality strategy, which selects the SD-WAN member with the best measured quality based on performance SLA metrics. The second rule uses the manual strategy, which specifies port1 as the SD-WAN member to select. Therefore, if an internal user pings 10.1.100.2 and 10.1.100.22 from subnet 172.16.205.0/24, the outgoing interfaces will be port16 and port1 respectively, assuming that port16 has the best quality among the SD-WAN members. References: https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/218559/configuring-the-sd-wan-interface

Question 3

Question Type: MultipleChoice

Refer to the exhibits.



Topology

Configuration

```
FGT-HA-1 # get system ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 1:35:12
```

The exhibits show a FortiGate network topology and the output of the status of high availability on the FortiGate.

Given this information, which statement is correct?

Options:

A- The ethertype values of the HA packets are 0x8890, 0x8891, and 0x8892

B- The cluster mode can support a maximum of four (4) FortiGate VMs

C- The cluster members are on the same network and the IP addresses were statically assigned.

D- FGVMEVLQOG33WM3D and FGVMEVGCJNHFYI4A share a virtual MAC address.

Answer:

D

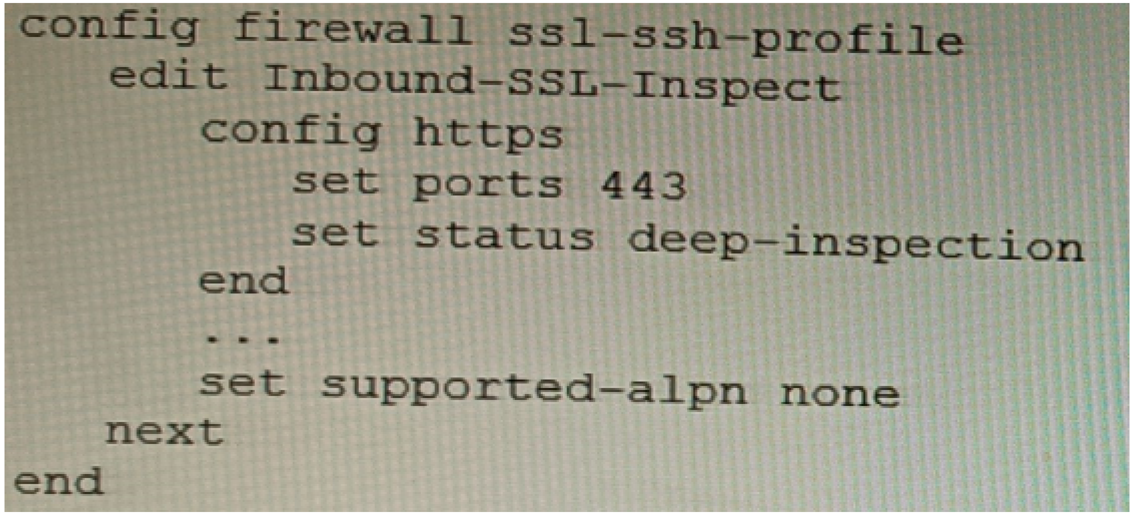
Explanation:

The output of the status of high availability on the FortiGate shows that the cluster mode is active-passive, which means that only one FortiGate unit is active at a time, while the other unit is in standby mode. The active unit handles all traffic and also sends HA heartbeat packets to monitor the standby unit. The standby unit becomes active if it stops receiving heartbeat packets from the active unit, or if it receives a higher priority from another cluster unit. In active-passive mode, all cluster units share a virtual MAC address for each interface, which is used as the source MAC address for all packets forwarded by the cluster. References: https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103439/high-availability-with-two-fortigates

Question 4

Question Type: MultipleChoice

Refer to the CLI configuration of an SSL inspection profile from a FortiGate device configured to protect a web server:



```
config firewall ssl-ssh-profile
    edit Inbound-SSL-Inspect
        config https
            set ports 443
            set status deep-inspection
        end
        ...
        set supported-alpn none
    next
end
```

Based on the information shown, what is the expected behavior when an HTTP/2 request comes in?

Options:

A- FortiGate will reject all HTTP/2 ALPN headers.

B- FortiGate will strip the ALPN header and forward the traffic.

C- FortiGate will rewrite the ALPN header to request HTTP/1.

D- FortiGate will forward the traffic without modifying the ALPN header.

Answer:

A

Explanation:

The supported-alpn parameter is set to http1.1 in the SSL inspection profile. This means that the FortiGate will only accept HTTP/1.1 traffic. Any HTTP/2 traffic will be rejected.

The following is the relevant documentation from Fortinet:

The supported-alpn parameter specifies the list of ALPN protocols that the FortiGate will accept. If the client requests a protocol that is not in this list, the FortiGate will reject the connection.

The default value for the supported-alpn parameter is all. This means that the FortiGate will accept any ALPN protocol that the client requests.

To reject all HTTP/2 traffic, set the supported-alpn parameter to http1.1.

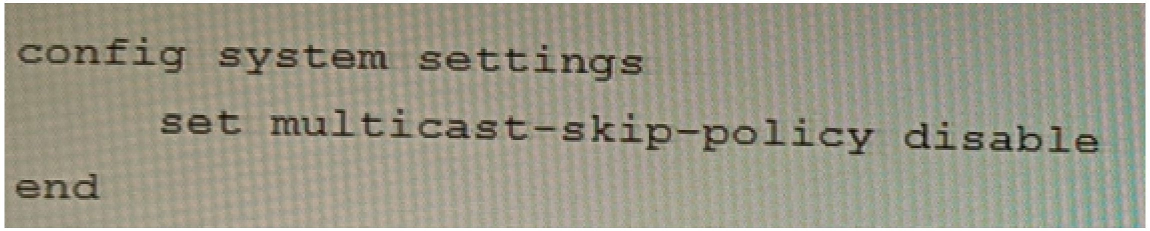
Source: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2-support-in-proxy-mode-ssl-inspection

Question 5

Question Type: **MultipleChoice**

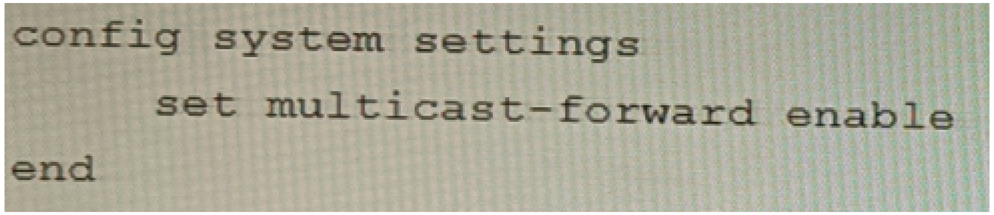
On a FortiGate Configured in Transparent mode, which configuration option allows you to control Multicast traffic passing through the?

A)



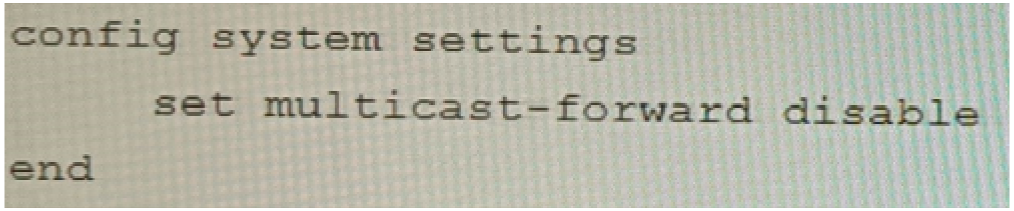
```
config system settings
      set multicast-skip-policy disable
end
```

B)



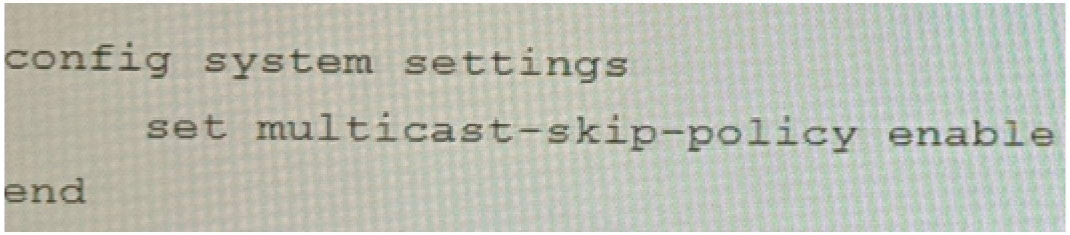
```
config system settings
      set multicast-forward enable
end
```

C)



```
config system settings
      set multicast-forward disable
end
```

D)



```
config system settings
      set multicast-skip-policy enable
end
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

C

Explanation:

To control multicast traffic passing through a FortiGate configured in transparent mode, you can use multicast policies. Multicast policies allow you to filter multicast traffic based on source and destination addresses, protocols, and interfaces. You can also apply security profiles to scan multicast traffic for threats and violations. References: https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/968606/configuring-multicast-forwarding

Question 6

Question Type: **MultipleChoice**

A remote worker requests access to an SSH server inside the network. You deployed a ZTNA Rule to their FortiClient. You need to follow the security requirements to inspect this traffic.

Which two statements are true regarding the requirements? (Choose two.)

Options:

A- FortiGate can perform SSH access proxy host-key validation.

B- You need to configure a FortiClient SSL-VPN tunnel to inspect the SSH traffic.

C- SSH traffic is tunneled between the client and the access proxy over HTTPS

D- Traffic is discarded as ZTNA does not support SSH connection rules

Answer:

A, C

Explanation:

ZTNA supports SSH connection rules that allow remote workers to access SSH servers inside the network through an HTTPS tunnel between the client and the access proxy (FortiGate). The access proxy acts as an SSH client to connect to the real SSH server on behalf of the user, and performs host-key validation to verify the identity of the server. The user can use any SSH client that supports HTTPS proxy settings, such as PuTTY or OpenSSH. References: https://docs.fortinet.com/document/fortigate/7.0.0/ztna-deployment/899992/configuring-ztna-rules-to-control-access

Question 7

Question Type: MultipleChoice

Which two statements are correct on a FortiGate using the FortiGuard Outbreak Protection Service (VOS)? (Choose two.)

Options:

A- The FortiGuard VOS can be used only with proxy-base policy inspections.

B- If third-party AV database returns a match the scanned file is deemed to be malicious.

C- The antivirus database queries FortiGuard with the hash of a scanned file

D- The AV engine scan must be enabled to use the FortiGuard VOS feature

E- The hash signatures are obtained from the FortiGuard Global Threat Intelligence database.

Answer:

C, E

Explanation:

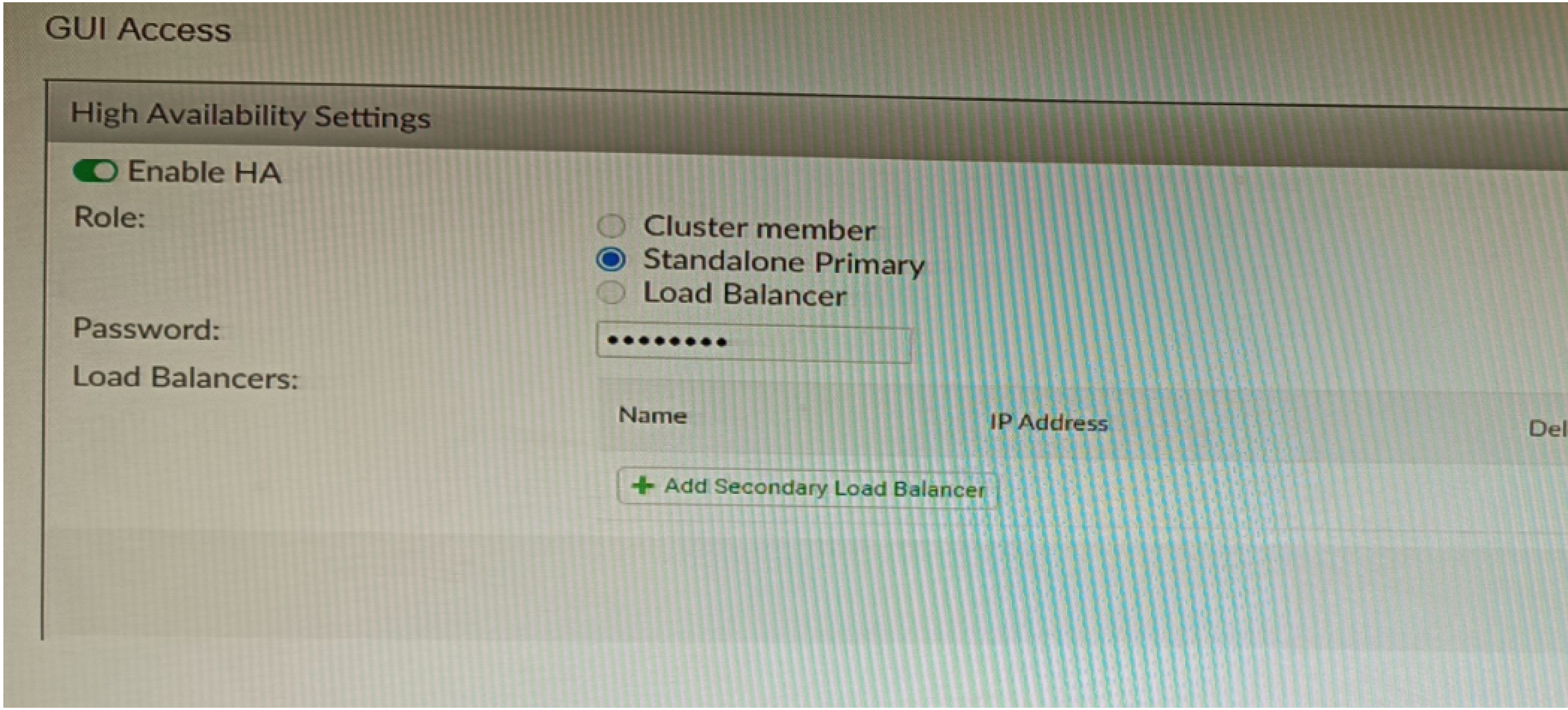
c) The antivirus database queries FortiGuard with the hash of a scanned file. This is how the FortiGuard VOS service works. The FortiGate queries FortiGuard with the hash of a scanned file, and FortiGuard returns a list of known malware signatures that match the hash.

e) The hash signatures are obtained from the FortiGuard Global Threat Intelligence database. This is where the FortiGuard VOS service gets its hash signatures from. The FortiGuard Global Threat Intelligence database is updated regularly with new malware signatures.

Question 8

Question Type: MultipleChoice

Refer to the exhibit, which shows the high availability configuration for the FortiAuthenticator (FAC1).



GUI Access

High Availability Settings

Enable HA

Role:

○ Cluster member

● Standalone Primary

○ Load Balancer

Password: •••••••••

Load Balancers:

Name	IP Address	Del

Based on this information, which statement is true about the next FortiAuthenticator (FAC2) member that will join an HA cluster with this FortiAuthenticator (FAC1)?

Options:

A- FAC2 can only process requests when FAC1 fails.

B- FAC2 can have its HA interface on a different network than FAC1.

C- The FortiToken license will need to be installed on the FAC2.

D- FSSO sessions from FAC1 will be synchronized to FAC2.

Answer:

D

Explanation:

When FortiAuthenticator operates in cluster mode, it provides active-passive failover and synchronization of all configuration and data, including FSSO sessions, between the cluster members. Therefore, if FAC1 is the active unit and FAC2 is the standby unit, any FSSO sessions from FAC1 will be synchronized to FAC2. If FAC1 fails, FAC2 will take over the active role and continue to process the FSSO sessions. References: https://docs.fortinet.com/document/fortiauthenticator/6.1.2/administration-guide/122076/high-availability