Vendor: Fortinet

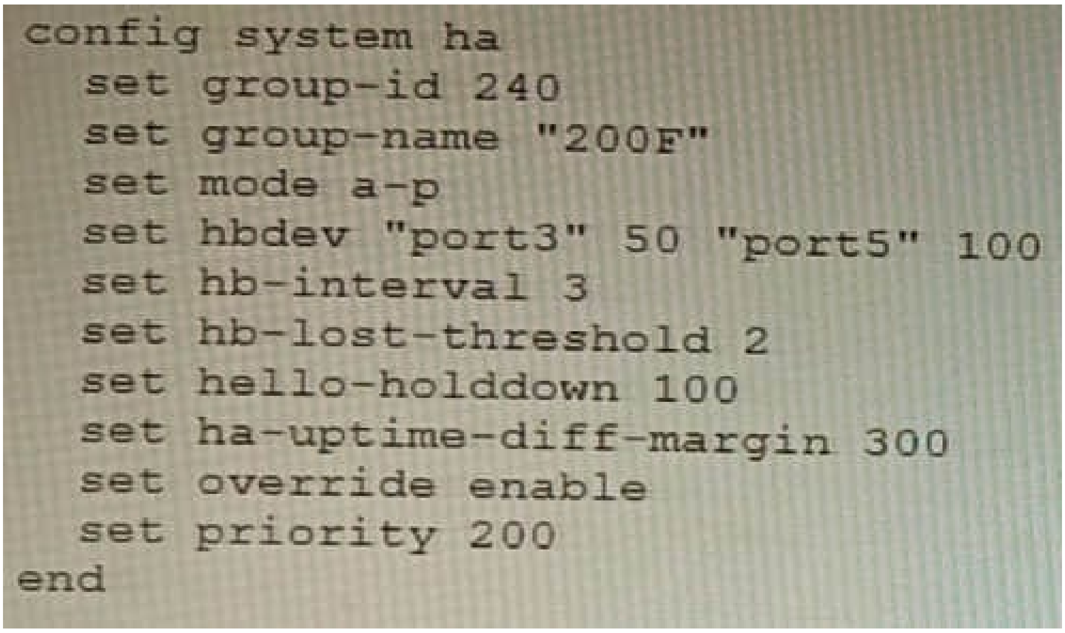
Exam Code:NSE8_812

Exam Name: Network Security Expert 8 Written Exam

Version: Demo

QUESTION 1

An HA topology is using the following configuration:



```
config system ha
   set group-id 240
   set group-name "200F"
   set mode a-p
   set hbdev "port3" 50 "port5" 100
   set hb-interval 3
   set hb-lost-threshold 2
   set hello-holddown 100
   set ha-uptime-diff-margin 300
   set override enable
   set priority 200
end
```

Based on this configuration, how long will it take for a failover to be detected by the secondary cluster member?

A. 600ms

B. 200ms

C. 300ms

D. 100ms

Correct Answer: B

Explanation: The HA heartbeat interval is 100ms, and the number of lost heartbeats before a failover is detected is 2. So, it will take 2 * 100ms = 200ms for a failover to be detected by the secondary cluster member.

Reference:

FortiGate High Availability:

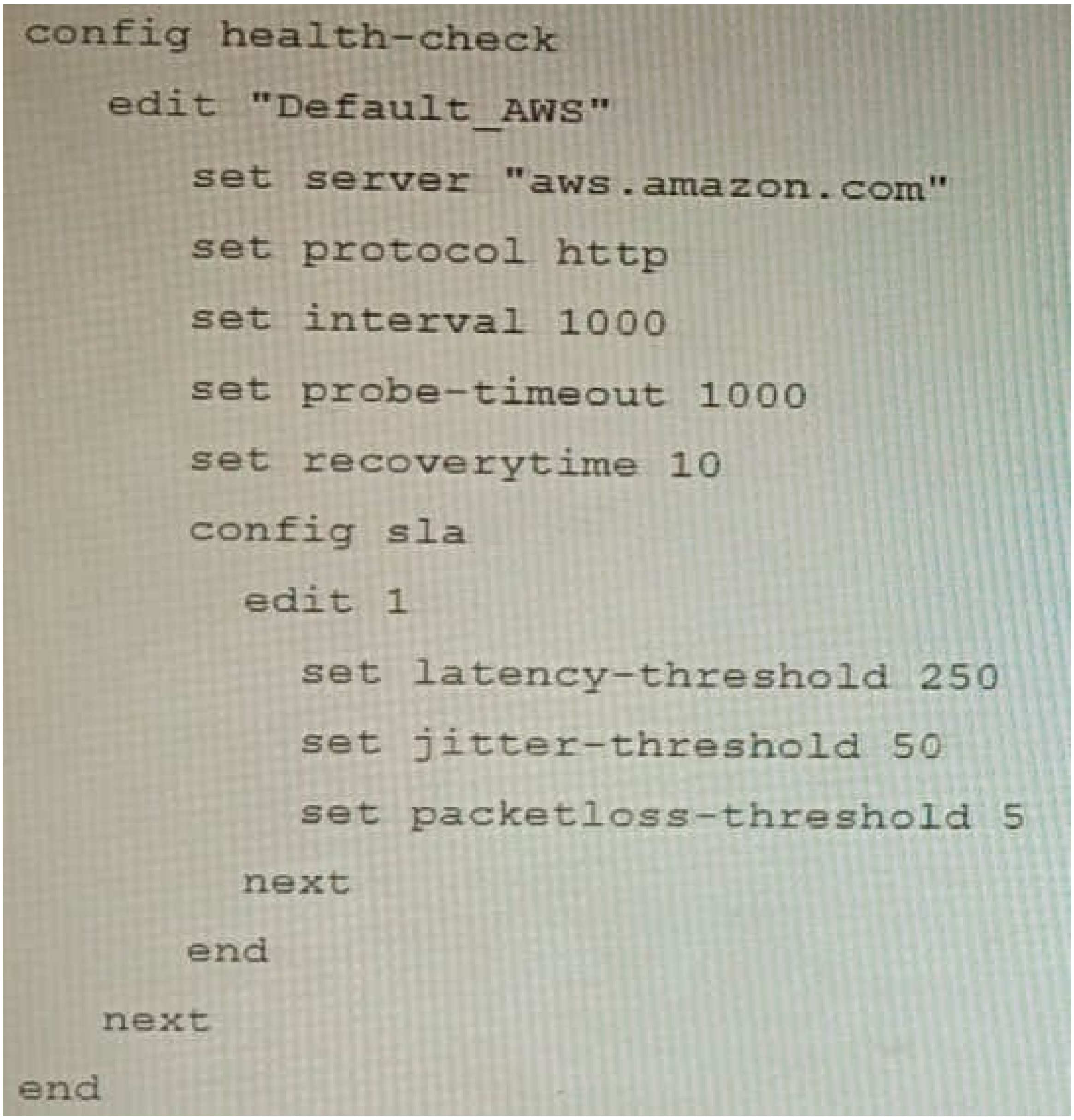
https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/647723/link- monitoring-and-ha-failover-time

---

QUESTION 2

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?

A. set members any

B. set members 0

C. current configuration already fulfills the requirement

D. set members all

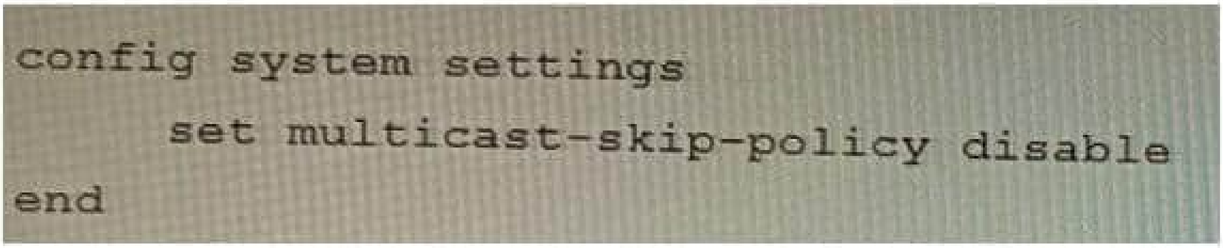
Correct Answer: A

Explanation: The set members any option will ensure that all of the SD-WAN interfaces are included in the Performance SLA. This is the best option if you want to be sure that the Performance SLA will be triggered even if more connections are added to the branch in the future. The set members 0 option will exclude all of the SD-WAN interfaces from the Performance SLA. This is not a good option because it will prevent the Performance SLA from being triggered even if there is a problem with the network. The current configuration already fulfills the requirement option is incorrect because it does not ensure that all of the SD-WAN interfaces will be included in the Performance SLA. The set members all option will include all of the SD-WAN interfaces in the Performance SLA, but it is not the best option because it is not scalable. If you have a large number of SD-WAN interfaces, this option will cause the Performance SLA to be triggered too often. References: Performance SLA | FortiGate / FortiOS 7.4.0 Configuring Performance SLA | FortiGate / FortiOS 7.4.0

QUESTION 3

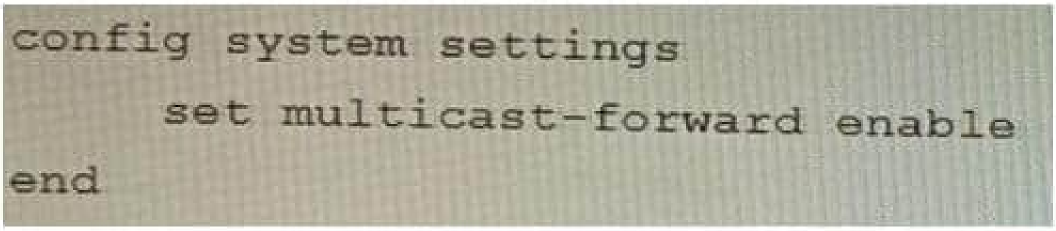
On a FortiGate Configured in Transparent mode, which configuration option allows you to control Multicast traffic passing through the?

○ A.



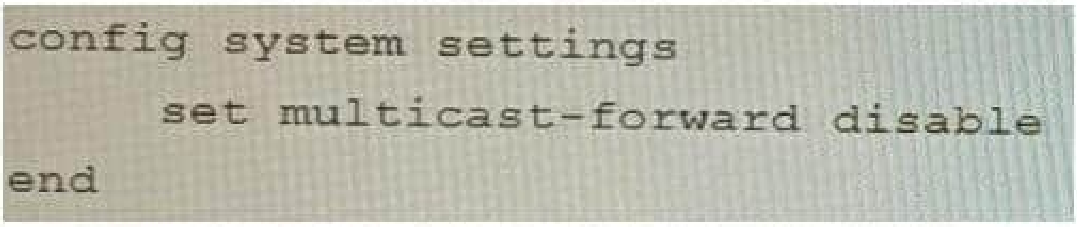
```
config system settings
      set multicast-skip-policy disable
end
```

○ B.



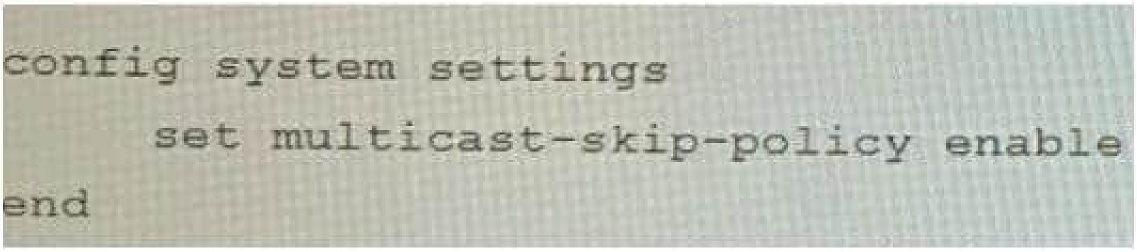
```
config system settings
      set multicast-forward enable
end
```

○ C.



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

○ D.



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

A. Option A

B. Option B

C. Option C

D. Option D

Correct 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 securityprofiles to scan multicast traffic for threats and violations.

References:https://docs.fortinet.com/document/fortigate/6.2.14/cookbook/968606/configurin g-multicast-forwarding

---

QUESTION 4

You are responsible for recommending an adapter type for NICs on a FortiGate VM that will run on an ESXi Hypervisor. Your recommendation must consider performance as the main concern, cost is not a factor. Which adapter type for the NICs will you recommend?

A. Native ESXi Networking with E1000

B. Virtual Function (VF) PCI Passthrough

C. Native ESXi Networking with VMXNET3

D. Physical Function (PF) PCI Passthrough

Correct Answer: C

Explanation: The FortiGate VM is a virtual firewall appliance that can run on various hypervisors, such as ESXi, Hyper-V, KVM, etc. The adapter type for NICs on a FortiGate VM determines the performance and compatibility of the network interface cards with the hypervisor and the physical network. There are different adapter types available for NICs on a FortiGate VM, such as E1000, VMXNET3, SR-IOV, etc. If performance is the main concern and cost is not a factor, one option is to use native ESXi networking with VMXNET3 adapter type for NICs on a FortiGate VM that will run on an ESXi hypervisor. VMXNET3 is a paravirtualized network interface card that is optimized for performance in virtual machines and supports features such as multiqueue support, Receive Side Scaling (RSS), Large Receive Offload (LRO), IPv6 offloads, and MSI/MSI-X interrupt delivery. Native ESXi networking means that the FortiGate VM uses the standard virtual switch (vSwitch) or distributed virtual switch (dvSwitch) provided by the ESXi hypervisor to connect to the physical network. This option can provide high performance and compatibility for NICs on a FortiGate VM without requiring additional hardware or software components. References:
https://docs.fortinet.com/document/fortigate/7.0.0/vm-installation- for-vmware-esxi/19662/installing-fortigate-vm-on-vmware- esxihttps://docs.fortinet.com/document/fortigate/7.0.0/vm-installationfor-vmware- esxi/19662/networking

---

QUESTION 5

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

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.

Correct Answer: CE

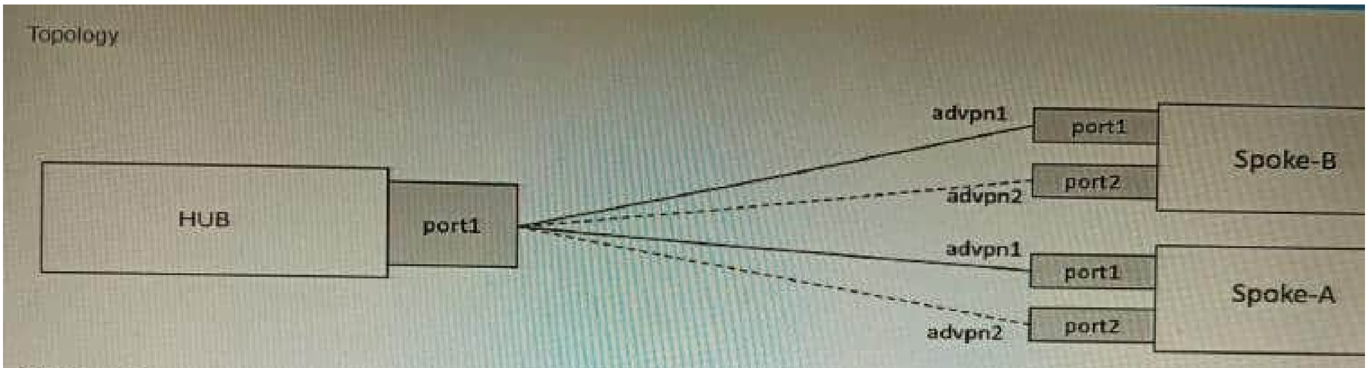
C. The antivirus database queries FortiGuard with the hash of a scanned file. This is how the FortiGuard VOS service works. The FortiGate queries FortiGuard with the hash of a scanned file, and FortiGuard returns a list of known malware signatures that match the hash.

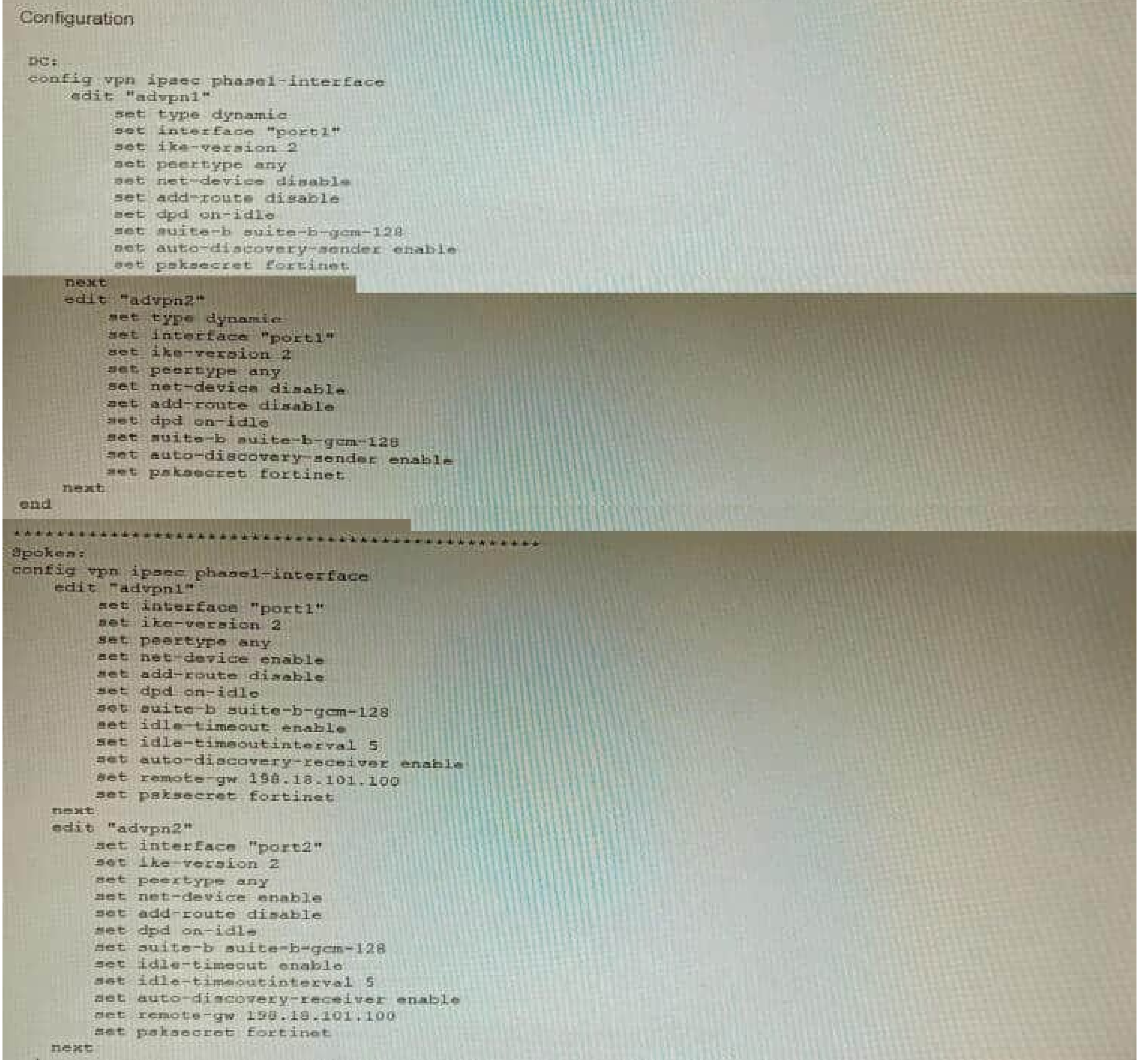
E. The hash signatures are obtained from the FortiGuard Global Threat Intelligence database. This is where the FortiGuard VOS service gets its hash signatures from. The FortiGuard Global Threat Intelligence database is updated regularly with new malware signatures.

QUESTION 6

Refer to the exhibits.

Topology





Configuration

```
DC:
config vpn ipsec phase1-interface
    edit "advpn1"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set add-route disable
        set dpd on-idle
        set suite-b suite-b-gcm-128
        set auto-discovery-sender enable
        set psksecret fortinet
    next
    edit "advpn2"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set add-route disable
        set dpd on-idle
        set suite-b suite-b-gcm-128
        set auto-discovery-sender enable
        set psksecret fortinet
    next
end
**************************************************
Spokes:
config vpn ipsec phase1-interface
    edit "advpn1"
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device enable
        set add-route disable
        set dpd on-idle
        set suite-b suite-b-gcm-128
        set idle-timeout enable
        set idle-timeoutinterval 5
        set auto-discovery-receiver enable
        set remote-gw 198.18.101.100
        set psksecret fortinet
    next
    edit "advpn2"
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device enable
        set add-route disable
        set dpd on-idle
        set suite-b suite-b-gcm-128
        set idle-timeout enable
        set idle-timeoutinterval 5
        set auto-discovery-receiver enable
        set remote-gw 198.18.101.100
        set psksecret fortinet
    next
```

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?

A. Use network-overlay id

B. Change advpn2 to IKEv1

C. Use local-id

D. Use peer-id

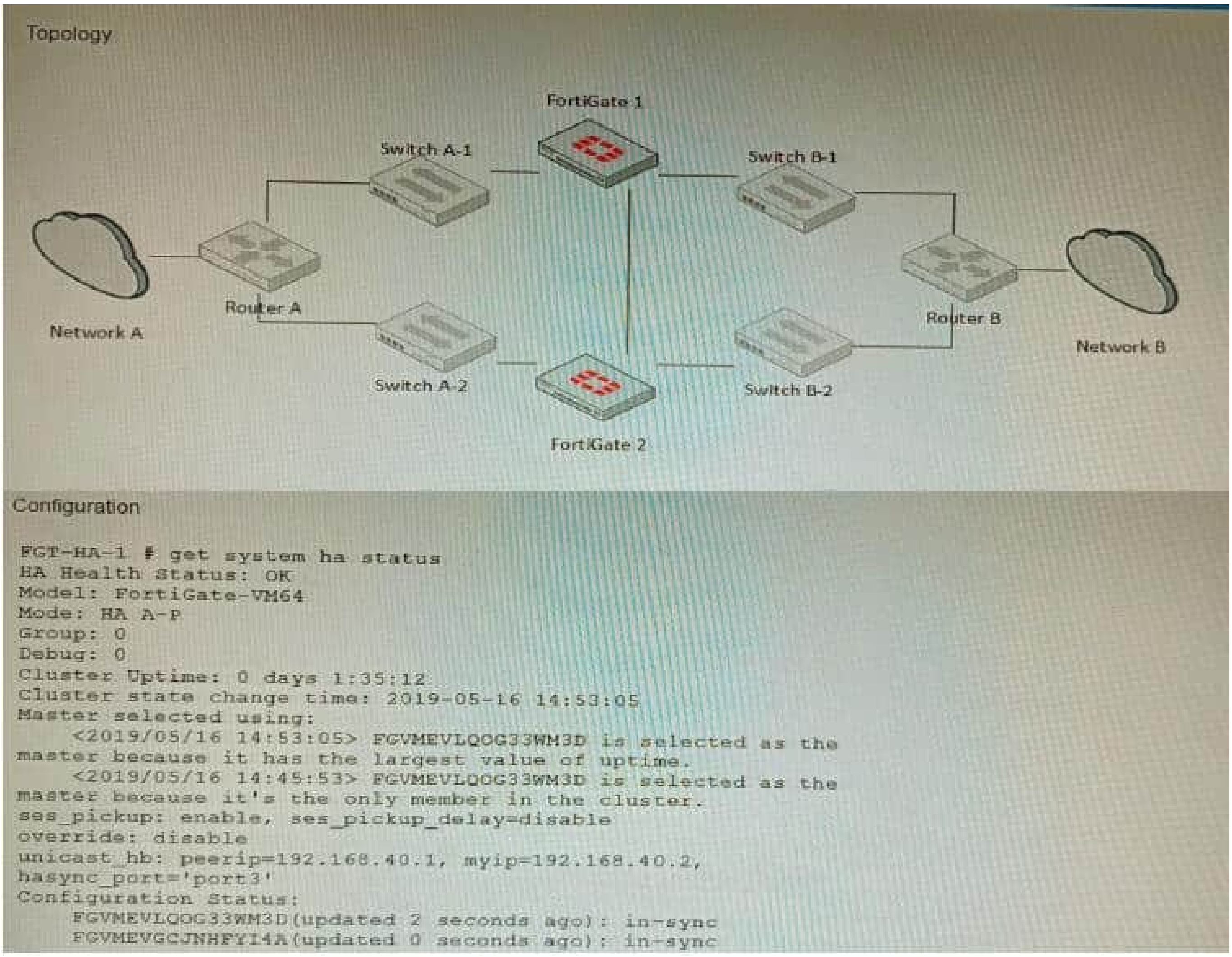
Correct Answer: A

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. References:
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 7

Refer to the exhibits.



```
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
Cluster state change time: 2019-05-16 14:53:05
Master selected using:
    <2019/05/16 14:53:05> FGVMEVLQOG33WM3D is selected as the
master because it has the largest value of uptime.
    <2019/05/16 14:45:53> FGVMEVLQOG33WM3D is selected as the
master because it's the only member in the cluster.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
unicast_hb: peerip=192.168.40.1, myip=192.168.40.2,
hasync_port='port3'
Configuration Status:
    FGVMEVLQOG33WM3D(updated 2 seconds ago): in-sync
    FGVMEVGCJNHFYI4A(updated 0 seconds ago): in-sync
```

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?

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.

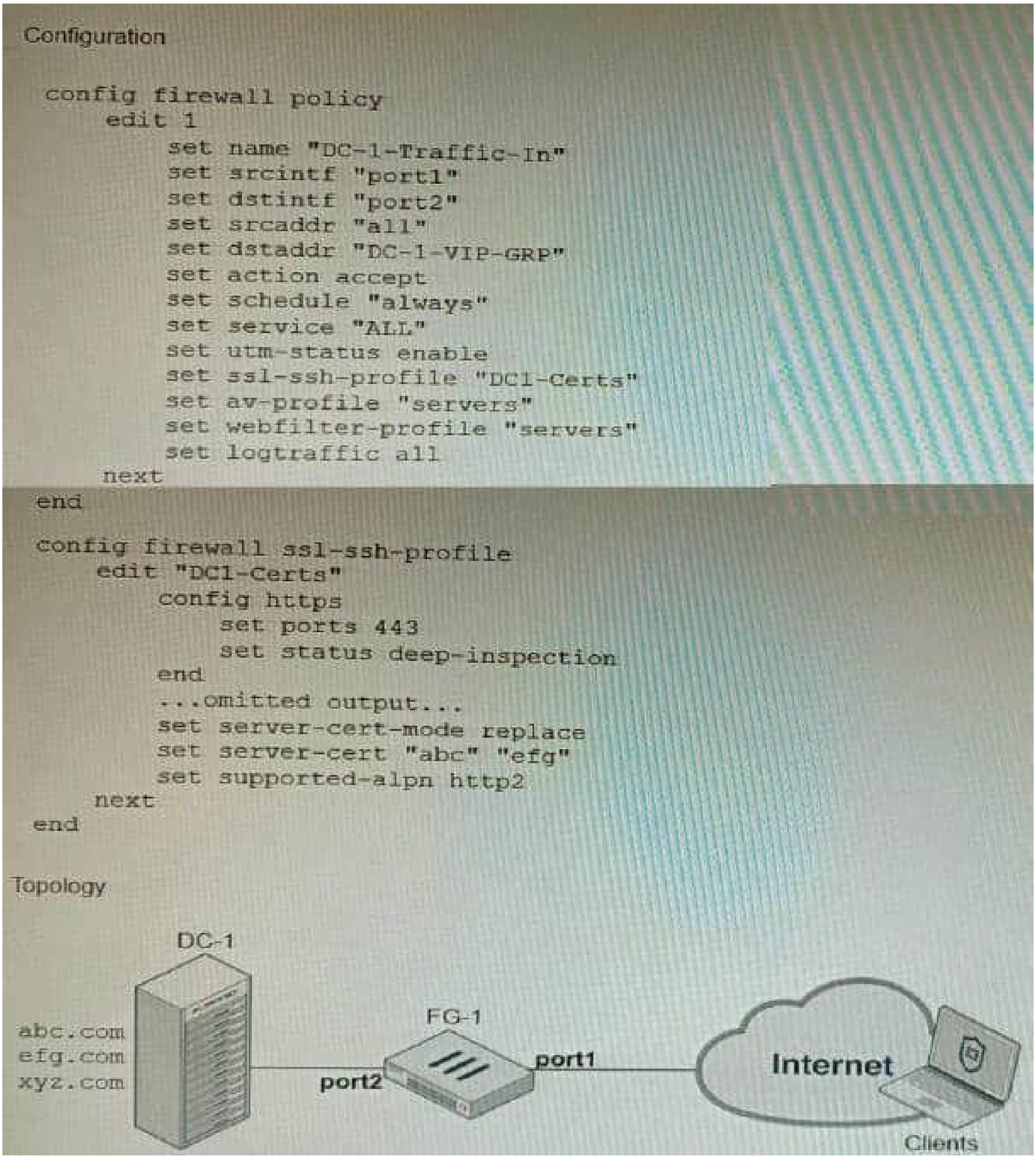
Correct Answer: D

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 8

Refer to the exhibits, which show a firewall policy configuration and a network topology.



Configuration

```
config firewall policy
    edit 1
        set name "DC-1-Traffic-In"
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "DC-1-VIP-GRP"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "DC1-Certs"
        set av-profile "servers"
        set webfilter-profile "servers"
        set logtraffic all
    next
end

config firewall ssl-ssh-profile
    edit "DC1-Certs"
        config https
            set ports 443
            set status deep-inspection
        end
        ...omitted output...
        set server-cert-mode replace
        set server-cert "abc" "efg"
        set supported-alpn http2
    next
end
```

Topology

An administrator has configured an inbound SSL inspection profile on a FortiGate device (FG-1) that is protecting a data center hosting multiple web pages-Given the scenario shown in the exhibits, which certificate will FortiGate use to handle requests to xyz.com?

A. FortiGate will fall-back to the default Fortinet_CA_SSL certificate.

B. FortiGate will reject the connection since no certificate is defined.

C. FortiGate will use the Fortinet_CA_Untrusted certificate for the untrusted connection,

D. FortiGate will use the first certificate in the server-cert list--the abc.com certificate

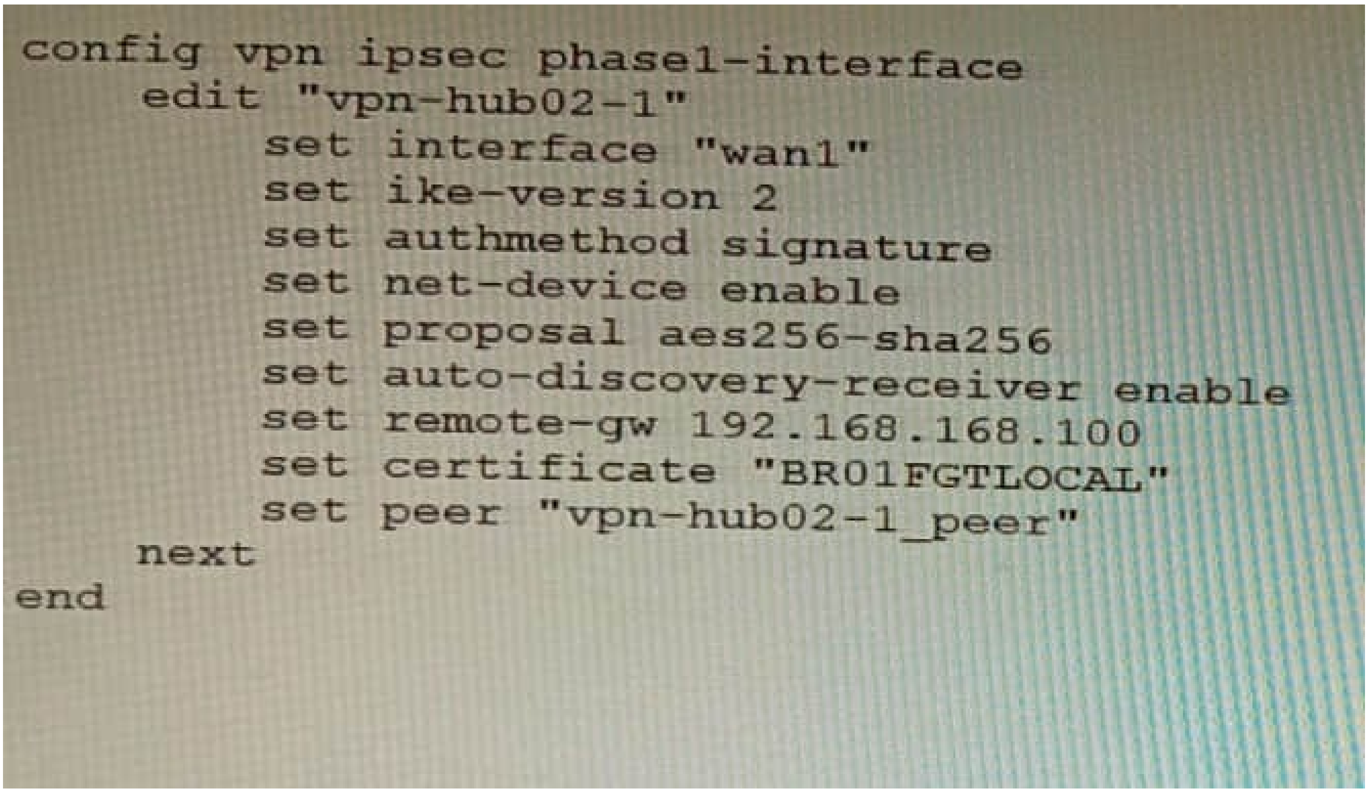
Correct Answer: A

Explanation: When using inbound SSL inspection, FortiGate needs to present a certificate to the client that matches the requested domain name. If no matching certificate is found in the server-cert list, FortiGate will fall-back to the default Fortinet_CA_SSL certificate, which is self-signed and may trigger a warning on the client browser.
References:https://docs.fortinet.com/document/fortigate/6.4.0/cookbook/103437/inbound- ssl-inspection

---

QUESTION 9

Refer to the exhibit.



```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set interface "wan1"
        set ike-version 2
        set authmethod signature
        set net-device enable
        set proposal aes256-sha256
        set auto-discovery-receiver enable
        set remote-gw 192.168.168.100
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

To facilitate a large-scale deployment of SD-WAN/ADVPN with FortiGate devices, you are tasked with configuring the FortiGate devices to support injecting of IKE routes on the ADVPN shortcut tunnels. Which three commands must be added or changed to the FortiGate spoke config vpn ipsec phasei-interface options referenced in the exhibit for the VPN interface to enable this capability? (Choose three.)

A. set net-device disable

B. set mode-cfg enable

C. set ike-version 1

D. set add-route enable

E. set mode-cfg-allow-client-selector enable

Correct Answer: BDE

B must be set to enable mode-cfg, which is required for injecting IKE routes on the ADVPN shortcut tunnels.

D must be set to enable add-route, which is the command that actually injects the IKE routes.

E must be set to enable mode-cfg-allow-client-selector, which allows custom phase 2 selectors to be configured.

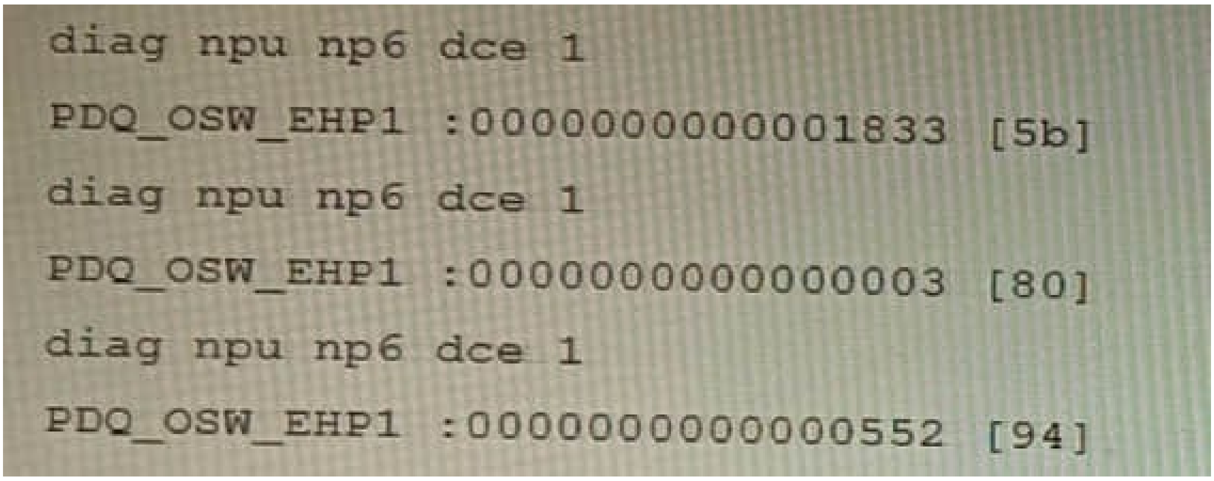
The other options are incorrect. Option A is incorrect because net-device disable is not required for injecting IKE routes on the ADVPN shortcut tunnels. Option C is incorrect because IKE version 1 is not supported for ADVPN.

References:

Phase 2 selectors and ADVPN shortcut tunnels | FortiGate / FortiOS 7.2.0 Configuring SD-WAN/ADVPN with FortiGate | FortiGate / FortiOS 7.2.0

QUESTION 10

You are running a diagnose command continuously as traffic flows through a platform with NP6 and you obtain the following output: Given the information shown in the output, which two statements are true? (Choose two.)



```
diag npu np6 dce 1
PDQ_OSW_EHP1 :0000000000001833 [5b]
diag npu np6 dce 1
PDQ_OSW_EHP1 :0000000000000003 [80]
diag npu np6 dce 1
PDQ_OSW_EHP1 :0000000000000552 [94]
```

A. Enabling bandwidth control between the ISF and the NP will change the output

B. The output is showing a packet descriptor queue accumulated counter

C. Enable HPE shaper for the NP6 will change the output

D. Host-shortcut mode is enabled.

E. There are packet drops at the XAUI.

Correct Answer: BE

Explanation: The diagnose command shown in the output is used to display information about NP6 packet descriptor queues. The output shows that there are 16 NP6 units in total, and each unit has four XAUI ports (XA0-XA3). The output also shows that there are some non-zero values in the columns PDQ ACCU (packet descriptor queue accumulated counter) and PDQ DROP (packet descriptor queue drop counter). These values indicate that there are some packet descriptor queues that have reached their maximum capacity and have dropped some packets at the XAUI ports. This could be caused by congestion or misconfiguration of the XAUI ports or the ISF (Internal Switch Fabric). References:https://docs.fortinet.com/document/fortigate/7.0.0/cli- reference/19662/diagnose-np6-pdq

The output is showing a packet descriptor queue accumulated counter, which is a measure of the number of packets that have been dropped by the NP6 due to congestion. The counter will increase if there are more packets than the NP6 can handle, which can happen if the bandwidth between the ISF and the NP is not sufficient or if the HPE shaper is enabled. The output also shows that there are packet drops at the XAUI, which is the interface between the NP6 and the FortiGate\\'s backplane. This means that the NP6 is not able to keep up with the traffic and is dropping packets. The other statements are not true. Host-shortcut mode is not enabled, and enabling bandwidth control between the ISF and the NP will not change the output. HPE shaper is a feature that can be enabled to improve performance, but it will not change the output of the diagnose command. Reference: https://docs.fortinet.com/document/fortigate/7.4.0/hardware-acceleration/48875/diagnose-npu-np6-dce-np6-id-number-of-dropped-np6-packets

---

QUESTION 11

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.)

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

Correct Answer: AD

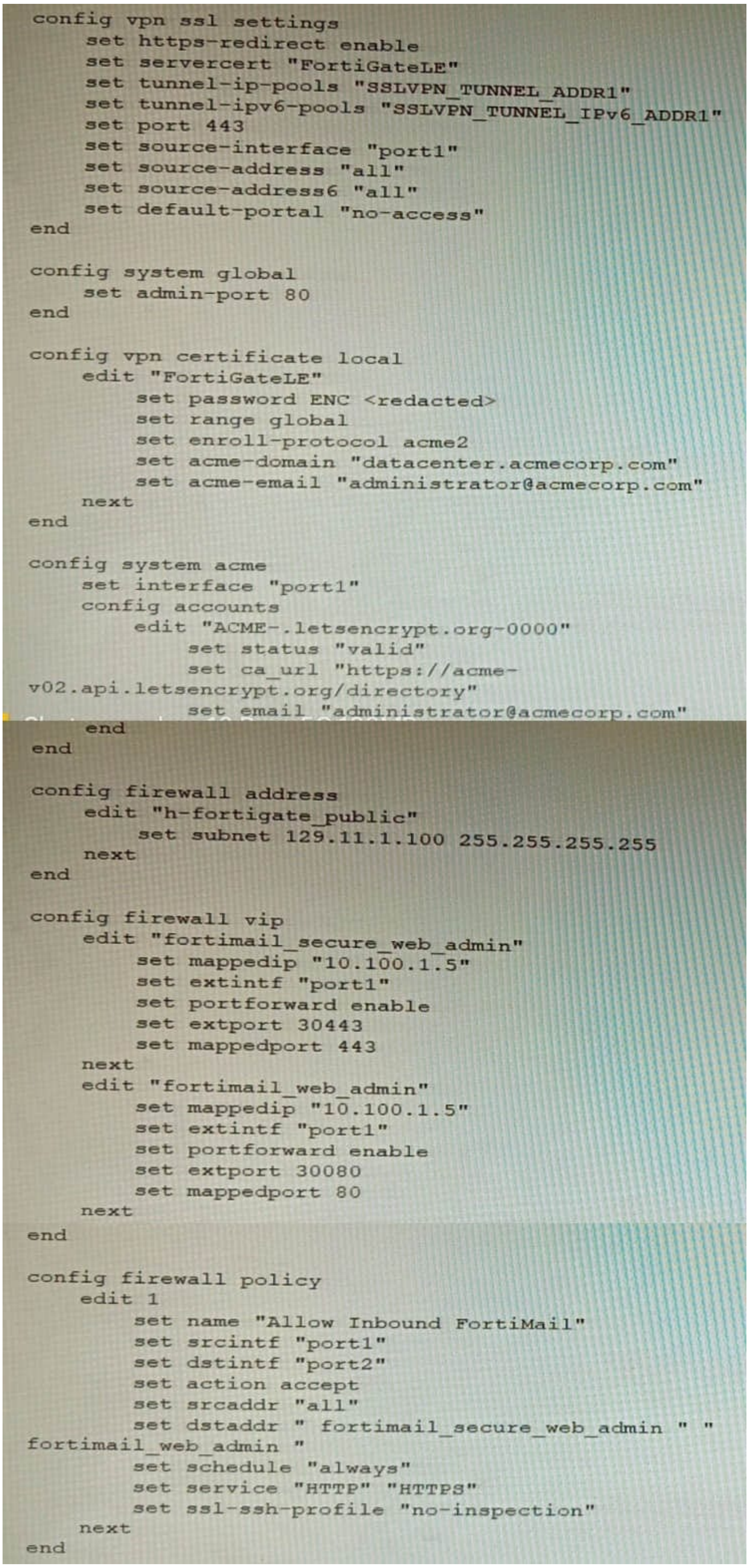
Explanation: To ensure that unnecessary multicast traffic is pruned from links that do not have a multicast listener, you must disable IGMP flood traffic on the ICL trunks and enable IGMP flood reports on the ISL and FortiLink trunks. Disabling

IGMP flood traffic will prevent the FortiSwitch units from flooding multicast traffic to all ports on the ICL trunks. This will help to reduce unnecessary multicast traffic on the network.

Enabling IGMP flood reports will allow the FortiSwitch units to learn which ports are interested in receiving multicast traffic. This will help the FortiSwitch units to prune multicast traffic from links that do not have a multicast listener.

QUESTION 12

Refer to the exhibit containing the configuration snippets from the FortiGate. Customer requirements: SSLVPN Portal must be accessible on standard HTTPS port (TCP/443) Public IP address (129.11.1.100) is assigned to portl Datacenter.acmecorp.com resolves to the public IP address assigned to portl

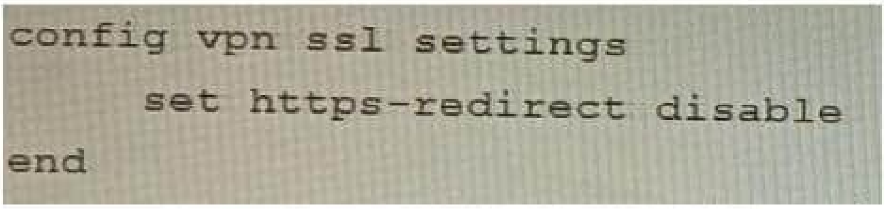


```
config vpn ssl settings
    set https-redirect enable
    set servercert "FortiGateLE"
    set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
    set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
    set port 443
    set source-interface "port1"
    set source-address "all"
    set source-address6 "all"
    set default-portal "no-access"
end

config system global
    set admin-port 80
end

config vpn certificate local
    edit "FortiGateLE"
        set password ENC <redacted>
        set range global
        set enroll-protocol acme2
        set acme-domain "datacenter.acmecorp.com"
        set acme-email "administrator@acmecorp.com"
    next
end

config system acme
    set interface "port1"
    config accounts
        edit "ACME-.letsencrypt.org-0000"
            set status "valid"
            set ca_url "https://acme-
v02.api.letsencrypt.org/directory"
            set email "administrator@acmecorp.com"
    end
end

config firewall address
    edit "h-fortigate_public"
        set subnet 129.11.1.100 255.255.255.255
    next
end

config firewall vip
    edit "fortimail_secure_web_admin"
        set mappedip "10.100.1.5"
        set extintf "port1"
        set portforward enable
        set extport 30443
        set mappedport 443
    next
    edit "fortimail_web_admin"
        set mappedip "10.100.1.5"
        set extintf "port1"
        set portforward enable
        set extport 30080
        set mappedport 80
    next
end

config firewall policy
    edit 1
        set name "Allow Inbound FortiMail"
        set srcintf "port1"
        set dstintf "port2"
        set action accept
        set srcaddr "all"
        set dstaddr " fortimail_secure_web_admin " "
fortimail_web_admin "
        set schedule "always"
        set service "HTTP" "HTTPS"
        set ssl-ssh-profile "no-inspection"
    next
end
```

The customer has a Let\\'s Encrypt certificate that is going to expire soon and it reports that subsequent attempts to renew that certificate are failing.

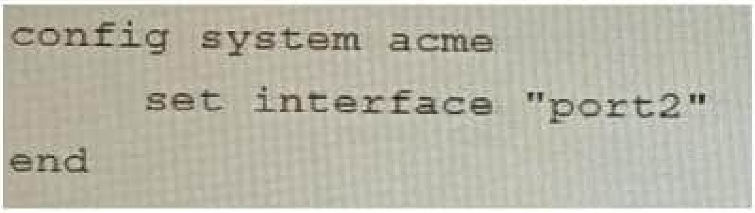
Reviewing the requirement and the exhibit, which configuration change below will resolve this issue?

○ A.



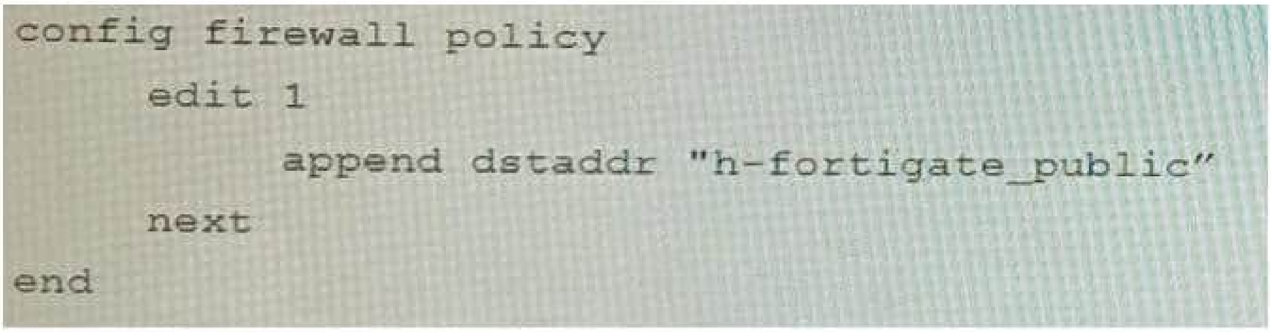
```
config vpn ssl settings
     set https-redirect disable
end
```

○ B.



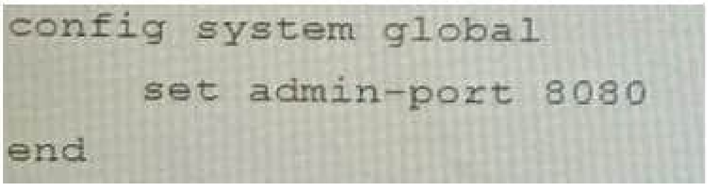
```
config system acme
     set interface "port2"
end
```

○ C.



```
config firewall policy
     edit 1
          append dstaddr "h-fortigate_public"
     next
end
```

○ D.



```
config system global
     set admin-port 8080
end
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

Explanation: The customer\\'s SSLVPN Portal is currently configured to use a self-signed certificate. This means that the certificate is not trusted by any browsers, and users will have to accept a security warning before they can connect to the

portal. To resolve this issue, the customer needs to configure the FortiGate to use a Let\\'s Encrypt certificate. Let\\'s Encrypt is a free certificate authority that provides trusted certificates for websites and other applications.

The configuration change in option B will configure the FortiGate to use a Let\\'s Encrypt certificate for the SSLVPN Portal. This will allow users to connect to the portal without having to accept a security warning.

The other configuration changes are not necessary to resolve the issue. Option A will configure the FortiGate to use a different port for the SSLVPN Portal, but this will not resolve the issue with the self-signed certificate. Option C will

configure the FortiGate to use a different DNS name for the SSLVPN Portal, but this will also not resolve the issue with the self-signed certificate. Option D will configure the FortiGate to use a different certificate authority for the SSLVPN

Portal, but this will also not resolve the issue because the customer still needs to use a trusted certificate.

References:

Configuring SSLVPN with Let\\'s Encrypt:

https://docs.fortinet.com/document/fortigate/7.0.0/administration- guide/822087/acme-certificate-support

Let\\'s Encrypt: https://letsencrypt.org/