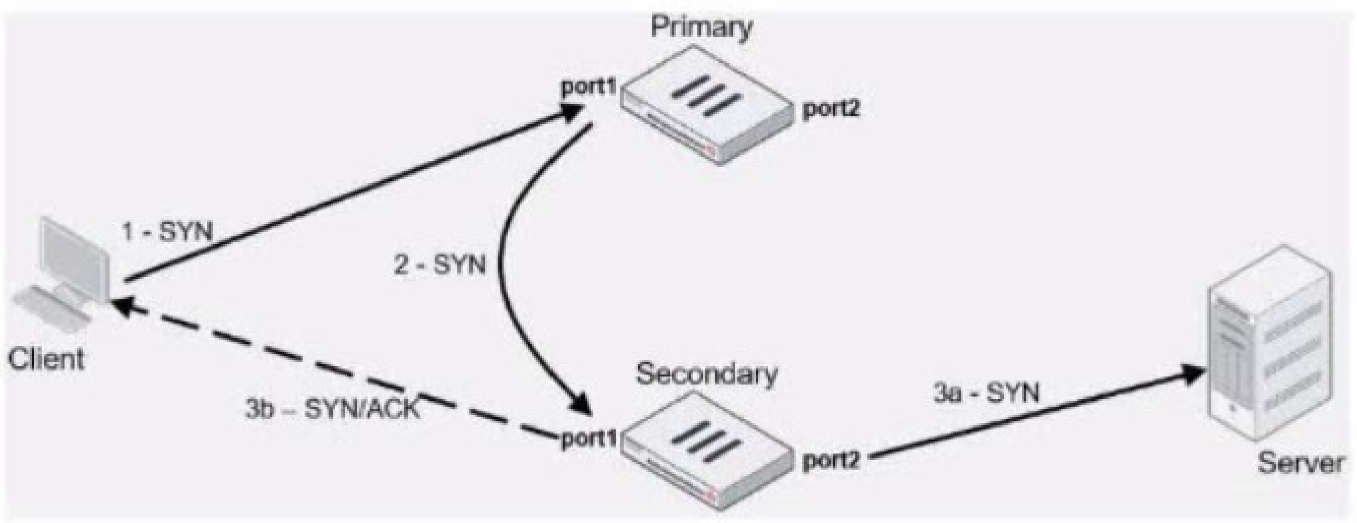
NSE7_EFW-7.2$^{Q\&As}$

Fortinet NSE 7 - Enterprise Firewall 7.2

Pass Fortinet NSE7_EFW-7.2 Exam with 100% Guarantee

QUESTION 1

Exhibit.



Refer to the exhibit, which contains an active-active toad balancing scenario.

During the traffic flow the primary FortiGate forwards the SYN packet to the secondary FortiGate.

What is the destination MAC address or addresses when packets are forwarded from the primary FortiGate to the secondary FortiGate?

A. Secondary physical MAC port1

B. Secondary virtual MAC port1

C. Secondary virtual MAC port1 then physical MAC port1

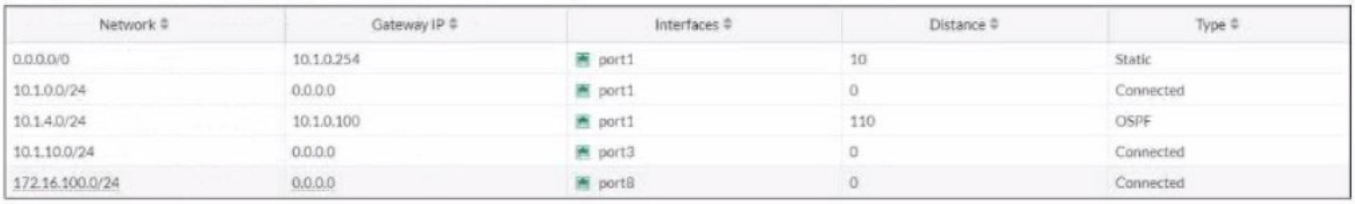
D. Secondary physical MAC port2 then virtual MAC port2

Correct Answer: A

In an active-active load balancing scenario, when the primary FortiGate forwards the SYN packet to the secondary FortiGate, the destination MAC address would be the secondary\\'s physical MAC on port1, as the packet is being sent over the network and the physical MAC is used for layer 2 transmissions.

QUESTION 2

Refer to the exhibit, which shows a routing table.



Network ⇕	Gateway IP ⇕	Interfaces ⇕	Distance ⇕	Type ⇕
0.0.0.0/0	10.1.0.254	port1	10	Static
10.1.0.0/24	0.0.0.0	port1	0	Connected
10.1.4.0/24	10.1.0.100	port1	110	OSPF
10.1.10.0/24	0.0.0.0	port3	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

What two options can you configure in OSPF to block the advertisement of the 10.1.10.0 prefix? (Choose two.)

A. Remove the 16.1.10.C prefix from the OSPF network

B. Configure a distribute-list-out

C. Configure a route-map out

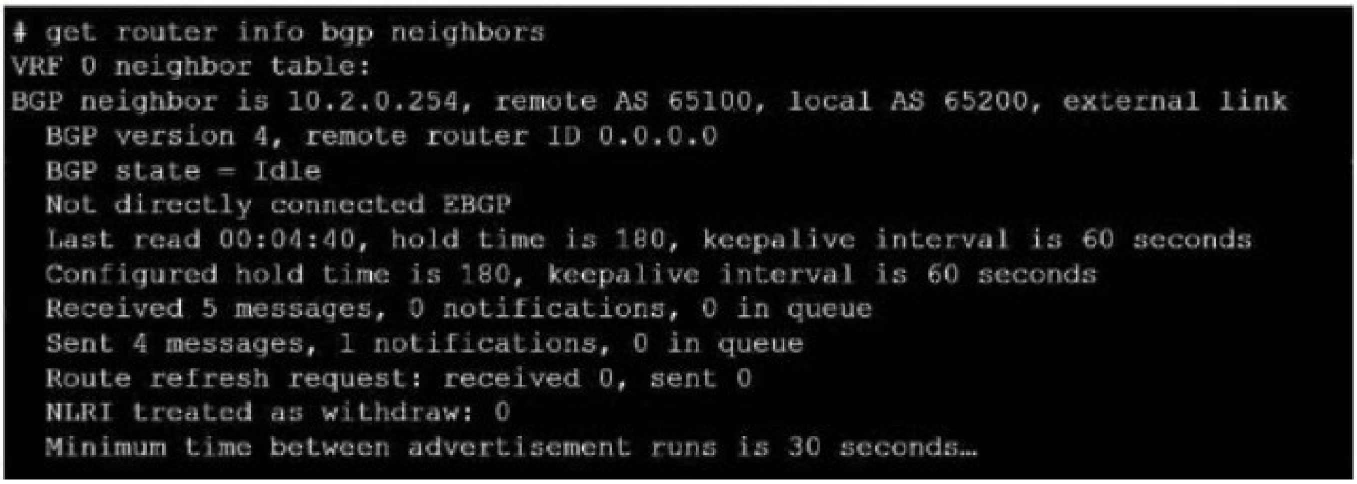
D. Disable Redistribute Connected

Correct Answer: BC

To block the advertisement of the 10.1.10.0 prefix in OSPF, you can configure a distribute-list-out or a route-map out. A distribute-list-out is used to filter outgoing routing updates from being advertised to OSPF neighbors1. A route-map out can also be used for filtering and is applied to outbound routing updates2. References := Technical Tip: Inbound route filtering in OSPF usi ... - Fortinet Community, OSPF | FortiGate / FortiOS 7.2.2 - Fortinet Documentation

QUESTION 3

Exhibit.



```
# get router info bgp neighbors
VRF 0 neighbor table:
BGP neighbor is 10.2.0.254, remote AS 65100, local AS 65200, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Not directly connected EBGP
  Last read 00:04:40, hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 180, keepalive interval is 60 seconds
  Received 5 messages, 0 notifications, 0 in queue
  Sent 4 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  NLRI treated as withdraw: 0
  Minimum time between advertisement runs is 30 seconds…
```

Refer to the exhibit, which provides information on BGP neighbors. Which can you conclude from this command output?

A. The router are in the number to match the remote peer.

B. You must change the AS number to match the remote peer.

C. BGP is attempting to establish a TCP connection with the BGP peer.

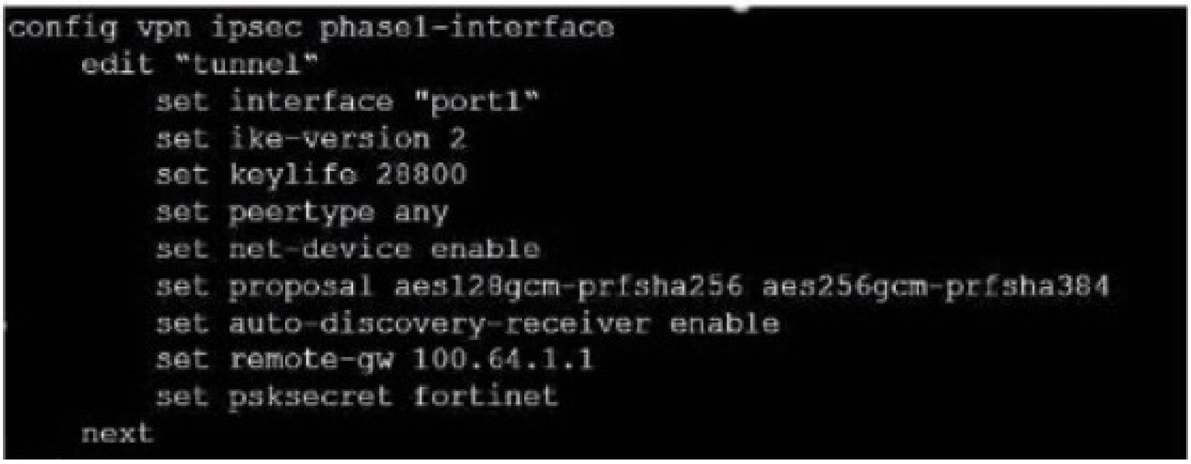
D. The bfd configuration to set to enable.

Correct Answer: C

The BGP state is "Idle", indicating that BGP is attempting to establish a TCP connection with the peer. This is the first state in the BGP finite state machine, and it means that no TCP connection has been established yet. If the TCP connection fails, the BGP state will reset to either active or idle, depending on the configuration. References: You can find more information about BGP states and troubleshooting in the following Fortinet Enterprise Firewall 7.2 documents: Troubleshooting BGP How BGP works

QUESTION 4

Exhibit.



```
config vpn ipsec phase1-interface
    edit "tunnel"
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device enable
        set proposal aes128gcm-prfsha256 aes256gcm-prfsha384
        set auto-discovery-receiver enable
        set remote-gw 100.64.1.1
        set psksecret fortinet
    next
```

Refer to the exhibit, which contains the partial ADVPN configuration of a spoke.

Which two parameters must you configure on the corresponding single hub? (Choose two.)

A. Set auto-discovery-sender enable

B. Set ike-version 2

C. Set auto-discovery-forwarder enable

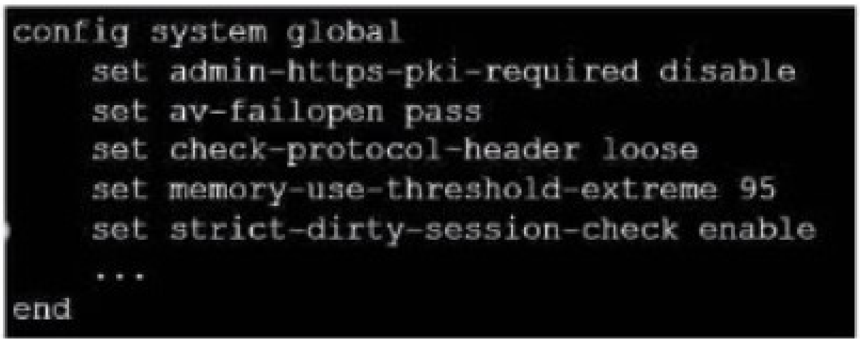
D. Set auto-discovery-receiver enable

Correct Answer: AC

For an ADVPN spoke configuration shown, the corresponding hub must have auto-discovery-senderenabled to send shortcut advertisement messages to the spokes. Also, the hub would need to haveauto-discovery-forwarderenabled if it is to forward on those shortcut advertisements to other spokes. This allows the hub to inform all spokes about the best path to reach each other. Theike-versiondoes not need to be reconfigured on the hub if it\\'s already set to version 2 andautodiscovery-receiveris not necessary on the hub because it\\'s the one sending the advertisements, not receiving. References: FortiOS Handbook - ADVPN

QUESTION 5

Refer to the exhibit.



```
config system global
    set admin-https-pki-required disable
    set av-failopen pass
    set check-protocol-header loose
    set memory-use-threshold-extreme 95
    set strict-dirty-session-check enable
    ...
end
```

which contains a partial configuration of the global system. What can you conclude from this output?

A. NPs and CPs are enabled

B. Only CPs arc disabled

C. Only NPs are disabled

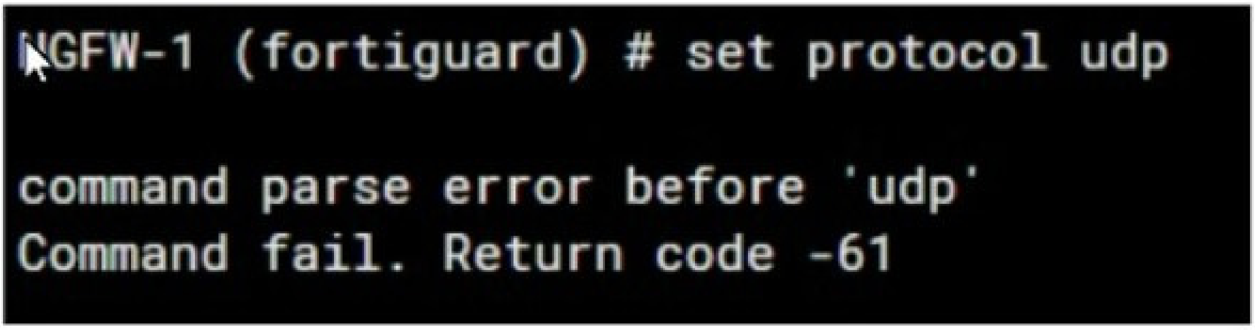
D. NPs and CPs arc disabled

Correct Answer: D

The configuration output shows various global settings for a FortiGate device. The terms NP (Network Processor) and CP (Content Processor) relate to FortiGate\\'s hardware acceleration features. However, the provided configuration output does not directly mention the status (enabled or disabled) of NPs and CPs. Typically, the command to disable or enable hardware acceleration features would specifically mention NP or CP in the command syntax. Therefore, based on the output provided, we cannot conclusively determine the status of NPs and CPs, hence option D is the closest answer since the output does not confirm that they are enabled. References: FortiOS Handbook - CLI Reference for FortiOS 5.2

QUESTION 6

Refer to the exhibit, which shows an error in system fortiguard configuration.



```
NGFW-1 (fortiguard) # set protocol udp

command parse error before 'udp'
Command fail. Return code -61
```

What is the reason you cannot set the protocol to udp in config system fortiguard?

A. FortiManager provides FortiGuard.

B. fortiguard-anycast is set to enable.

C. You do not have the corresponding write access.

D. udp is not a protocol option.

Correct Answer: D

The reason for the command failure when trying to set the protocol to UDP in theconfig system fortiguardis likely that UDP is not a protocol option in this context. The command syntax might be incorrect or the option to set a protocol for FortiGuard updates might not exist in this manner. So the correct answer is D. udp is not a protocol option.

QUESTION 7

In which two ways does fortiManager function when it is deployed as a local FDS? (Choose two)

A. It can be configured as an update server a rating server or both

B. It provides VM license validation services

C. It supports rating requests from non-FortiGate devices.

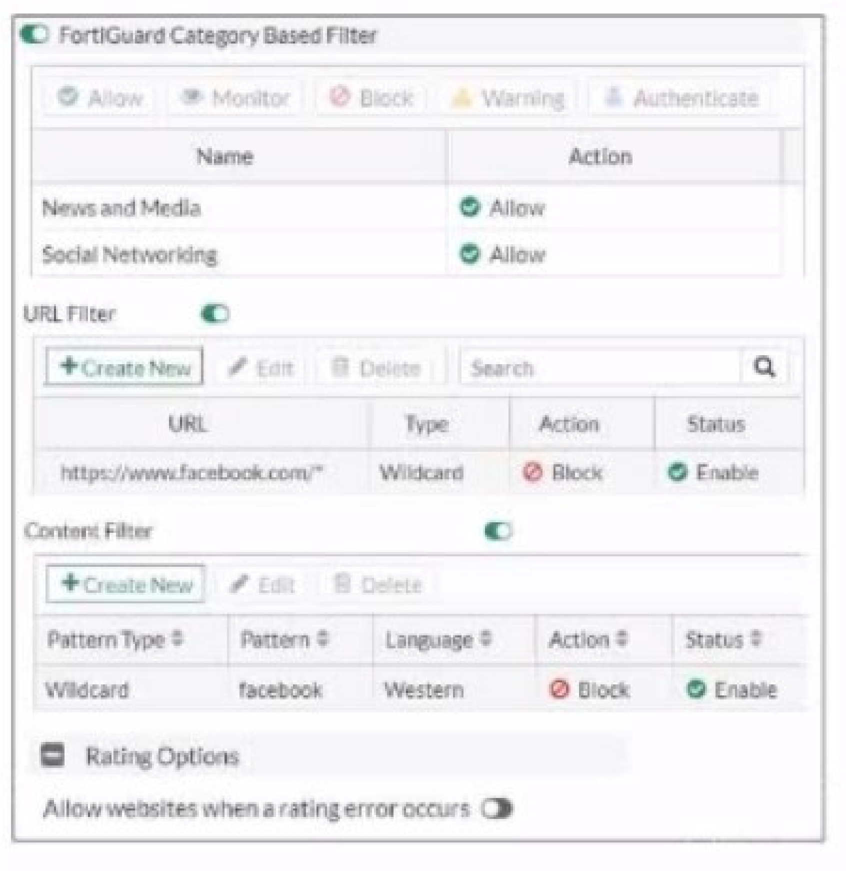
D. It caches available firmware updates for unmanaged devices

Correct Answer: AB

When deployed as a local FortiGuard Distribution Server (FDS), FortiManager functions in several capacities. It can act as an update server, a rating server, or both, providing firmware updates and FortiGuard database updates. Additionally, it plays a crucial role in VM license validation services, ensuring that the connected FortiGate devices are operating with valid licenses. However, it does not support rating requests from non-FortiGate devices nor cache firmware updates for unmanaged devices. Fortinet FortiOS Handbook: FortiManager as a Local FDS Configuration

QUESTION 8

Exhibit.



FortiGuard Category Based Filter

Name	Action
News and Media	✓ Allow
Social Networking	✓ Allow

URL Filter ●

URL	Type	Action	Status
https://www.facebook.com/*	Wildcard	⊘ Block	✓ Enable

Content Filter ●

Pattern Type	Pattern	Language	Action	Status
Wildcard	facebook	Western	⊘ Block	✓ Enable

Rating Options

Allow websites when a rating error occurs ○

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

What can you cone udo from this configuration about access towww.facebook, com, which is categorized as Social Networking?

A. The access is blocked based on the Content Filter configuration

B. The access is allowed based on the FortiGuard Category Based Filter configuration

C. The access is blocked based on the URL Filter configuration

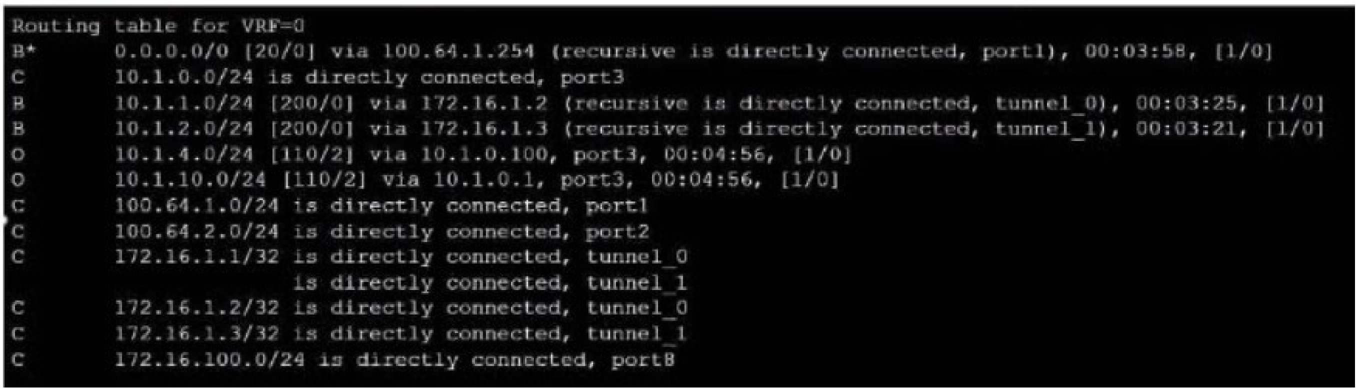
D. The access is hocked if the local or the public FortiGuard server does not reply

Correct Answer: C

The access to www.facebook.com is blocked based on the URL Filter configuration. In the exhibit, it shows that the URL "www.facebook.com" is specifically set to "Block" under the URL Filter section1. References := Fortigate: How to configure Web Filter function on Fortigate, Web filter | FortiGate / FortiOS 7.0.2 | Fortinet Document Library, FortiGate HTTPS web URL filtering ... - Fortinet ... - Fortinet Community

QUESTION 9

Exhibit.



```
Routing table for VRF=0
B*      0.0.0.0/0 [20/0] via 100.64.1.254 (recursive is directly connected, port1), 00:03:58, [1/0]
C       10.1.0.0/24 is directly connected, port3
B       10.1.1.0/24 [200/0] via 172.16.1.2 (recursive is directly connected, tunnel_0), 00:03:25, [1/0]
B       10.1.2.0/24 [200/0] via 172.16.1.3 (recursive is directly connected, tunnel_1), 00:03:21, [1/0]
O       10.1.4.0/24 [110/2] via 10.1.0.100, port3, 00:04:56, [1/0]
O       10.1.10.0/24 [110/2] via 10.1.0.1, port3, 00:04:56, [1/0]
C       100.64.1.0/24 is directly connected, port1
C       100.64.2.0/24 is directly connected, port2
C       172.16.1.1/32 is directly connected, tunnel_0
                      is directly connected, tunnel_1
C       172.16.1.2/32 is directly connected, tunnel_0
C       172.16.1.3/32 is directly connected, tunnel_1
C       172.16.100.0/24 is directly connected, port8
```

Refer to the exhibit, which shows a partial touting table

What two concisions can you draw from the corresponding FortiGate configuration? (Choose two.)

A. IPSec Tunnel aggregation is configured

B. net-device is enabled in the tunnel IPSec phase 1 configuration

C. OSPI is configured to run over IPSec.

D. add-route is disabled in the tunnel IPSec phase 1 configuration.

Correct Answer: BD

Option B is correct because the routing table shows that the tunnel interfaces have a netmask of 255.255.255.255, which indicates that net-device is enabled in the phase 1 configuration. This option allows the FortiGate to use the tunnel interface as a next-hop for routing, without adding a route to the phase 2 destination1. Option D is correct because the routing table does not show any routes to the phase 2 destination networks, which indicates that add-route is disabled in the phase 1 configuration. This option controls whether the FortiGate adds a static route to the phase 2 destination network using the tunnel interface as the gateway2. Option A is incorrect because IPSec tunnel aggregation is a feature that allows multiple phase 2 selectors to share a single phase 1 tunnel, reducing the number of tunnels and improving performance3. This feature is not related to the routing table or the phase 1 configuration. Option C is incorrect because OSPF is a dynamic routing protocol that can run over IPSec tunnels, but it requires additional configuration on the FortiGate and the peer device4. This option is not related to the routing table or the phase 1 configuration. References: =

1: Technical Tip: `set net-device\\' new route-based IPsec logic2

2: Adding a static route5

3: IPSec VPN concepts6

4: Dynamic routing over IPsec VPN7

QUESTION 10

You contoured an address object on the tool fortiGate in a Security Fabric. This object is not synchronized with a downstream device. Which two reasons could be the cause? (Choose two)

A. The address object on the tool FortiGate has fabric-object set to disable

B. The root FortiGate has configuration-sync set to enable

C. The downstream TortiGate has fabric-object-unification set to local

D. The downstream FortiGate has configuration-sync set to local

Correct Answer: AC

Option A is correct because the address object on the tool FortiGate will not be synchronized with the downstream devices if it has fabric-object set to disable. This option controls whether the address object is shared with other FortiGate devices in the Security Fabric or not1. Option C is correct because the downstream FortiGate will not receive the address object from the tool FortiGate if it has fabric-object-unification set to local. This option controls whether the downstream FortiGate uses the address objects from the root FortiGate or its own local address objects2. Option B is incorrect because the root FortiGate has configuration-sync set to enable by default, which means that it will synchronize the address objects with the downstream devices unless they are disabled by the fabric-object option3. Option D is incorrect because the downstream FortiGate has configuration-sync set to local by default, which means that it will receive the address objects from the root FortiGate unless they are overridden by the fabric-object-unification option4. References: =

1: Group address objects synchronized from FortiManager5

2: Security Fabric address object unification6

3: Configuration synchronization7

4: Configuration synchronization7 : Security Fabric - Fortinet Documentation