Free Questions for NSE7_EFW-7.2 by vceexamstest

Shared by Foley on 15-04-2024

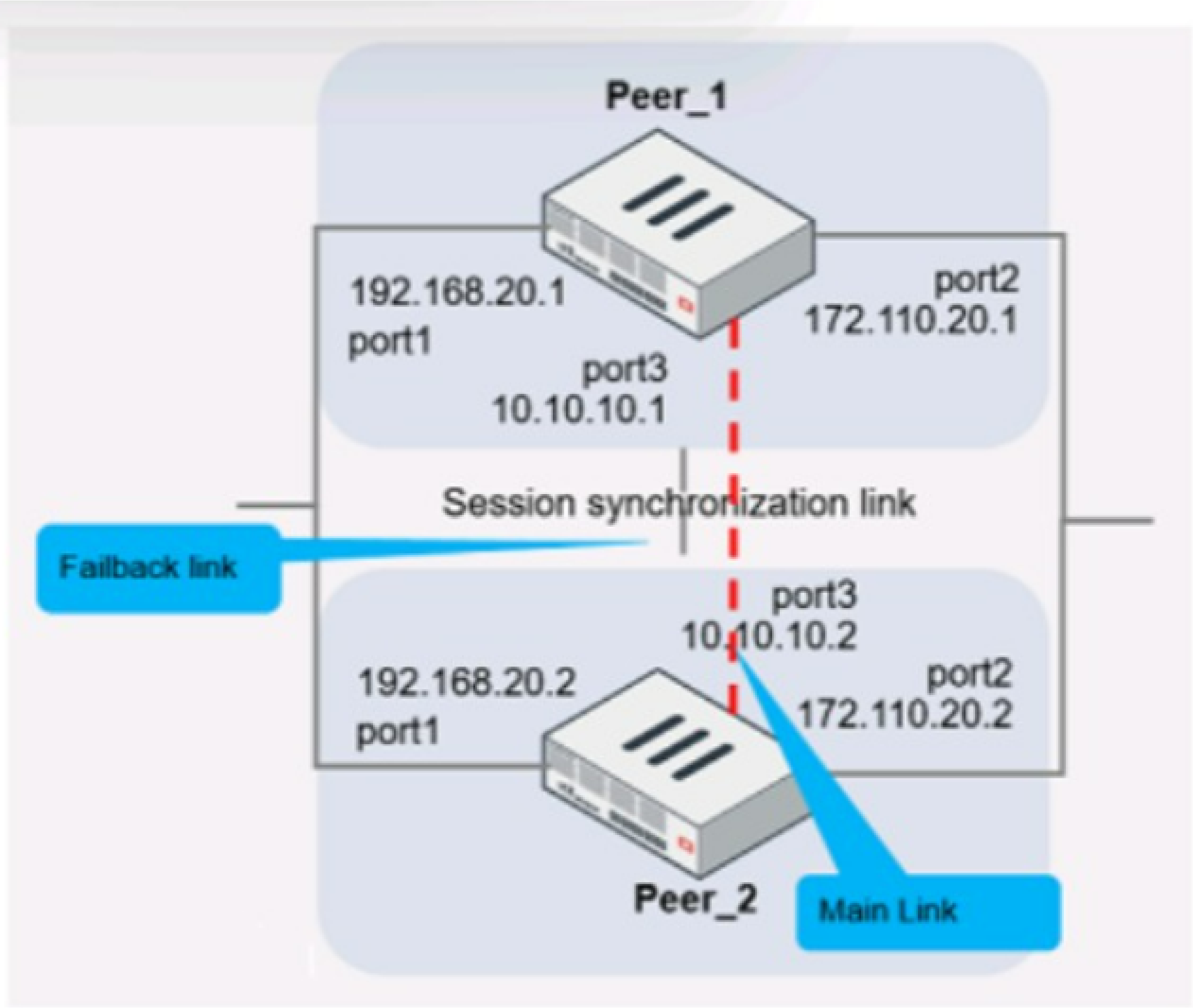
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit, which shows two configured FortiGate devices and peering over FGSP.



The main link directly connects the two FortiGate devices and is configured using the set session-syn-dev command.

What is the primary reason to configure the main link?

Options:

A- To have both sessions and configuration synchronization in layer 2

B- To load balance both sessions and configuration synchronization between layer 2 and 3

C- To have only configuration synchronization in layer 3

D- To have both sessions and configuration synchronization in layer 3

Answer:

D

Explanation:

The primary purpose of configuring a main link between the devices is to synchronize session information so that if one unit fails, the other can continue processing traffic without dropping active sessions.

A. To have both sessions and configuration synchronization in layer 2. This is incorrect because FGSP is used for session synchronization, not configuration synchronization.

B. To load balance both sessions and configuration synchronization between layer 2 and 3. FGSP does not perform load balancing and is not used for configuration synchronization.

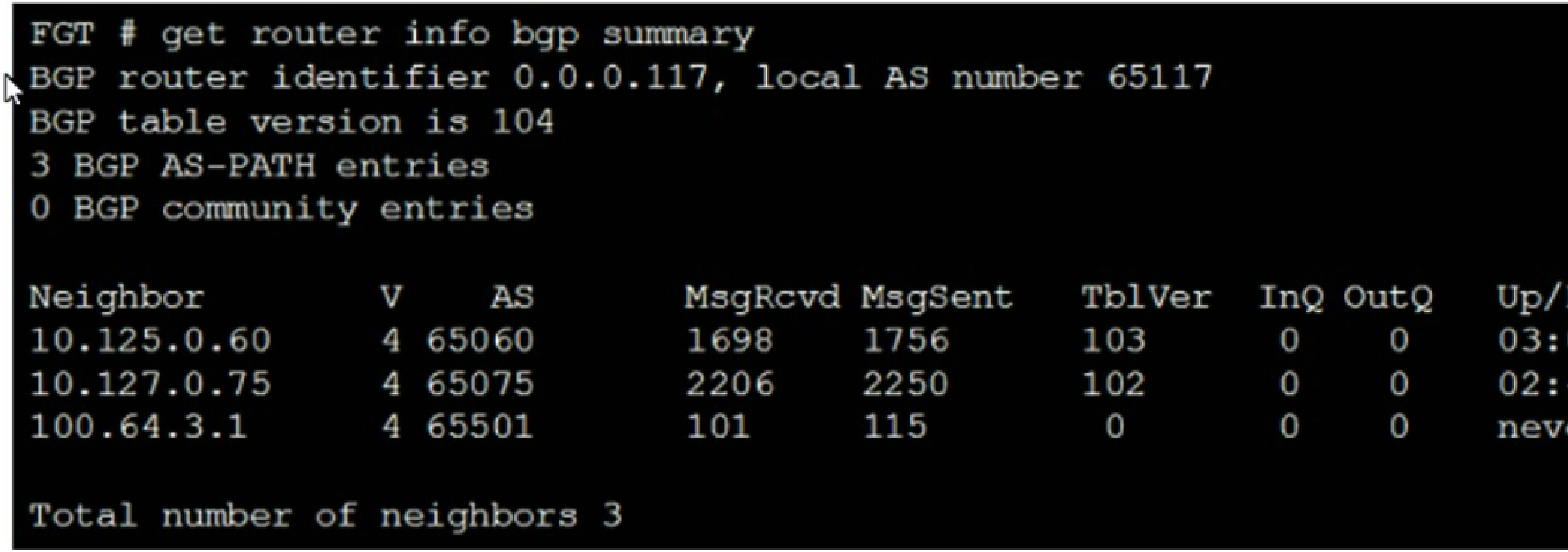
C. To have only configuration synchronization in layer 3. The main link is not used solely for configuration synchronization.

D. To have both sessions and configuration synchronization in layer 3. The main link in an FGSP setup is indeed used to synchronize session information across the devices, and it operates at layer 3 since it uses IP addresses to establish the peering.

Question 2

Question Type: MultipleChoice

Refer to the exhibit, which shows the output of a BGP summary.



```
FGT # get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS      MsgRcvd MsgSent   TblVer  InQ OutQ  Up/
10.125.0.60     4 65060      1698    1756      103       0    0  03:
10.127.0.75     4 65075      2206    2250      102       0    0  02:
100.64.3.1      4 65501      101     115         0       0    0  nev

Total number of neighbors 3
```

What two conclusions can you draw from this BGP summary? (Choose two.)

Options:

A- External BGP (EBGP) exchanges routing information.

B- The BGP session with peer 10. 127. 0. 75 is established.

C- The router 100. 64. 3. 1 has the parameter bfd set to enable.

D- The neighbors displayed are linked to a local router with the neighbor-range set to a value of 4.

Answer:

A, B

Explanation:

The output of the BGP (Border Gateway Protocol) summary shows details about the BGP neighbors of a router, their Autonomous System (AS) numbers, the state of the BGP session, and other metrics like messages received and sent.

From the BGP summary provided:

A. External BGP (EBGP) exchanges routing information. This conclusion can be inferred because the AS numbers for the neighbors are different from the local AS number (65117), which suggests that these are external connections.

B. The BGP session with peer 10.127.0.75 is established. This is indicated by the state/prefix received column showing a numeric value (1), which typically means that the session is established and a number of prefixes has been received.

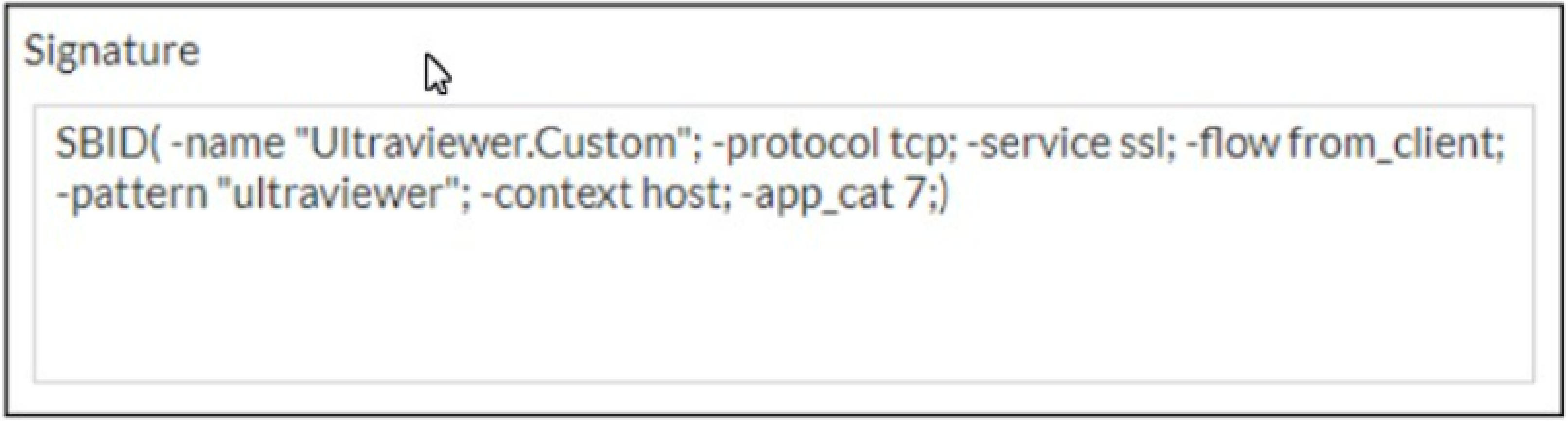
C. The router 100.64.3.1 has the parameter bfd set to enable. This cannot be concluded directly from the summary without additional context or commands specifically showing BFD (Bidirectional Forwarding Detection) configuration.

D. The neighbors displayed are linked to a local router with the neighbor-range set to a value of 4. The neighbor-range concept does not apply here; the value 4 in the 'V' column stands for the BGP version number, which is typically 4.

Question 3

Question Type: **MultipleChoice**

Refer to the exhibit, which shows a custom signature.



Signature

```
SBID( -name "Ultraviewer.Custom"; -protocol tcp; -service ssl; -flow from_client;
-pattern "ultraviewer"; -context host; -app_cat 7;)
```

Which two modifications must you apply to the configuration of this custom signature so that you can save it on FortiGate? (Choose two.)

Options:

A- Add severity.

B- Add attack_id.

C- Ensure that the header syntax is F-SBID.

D- Start options with --.

Answer:

A, B

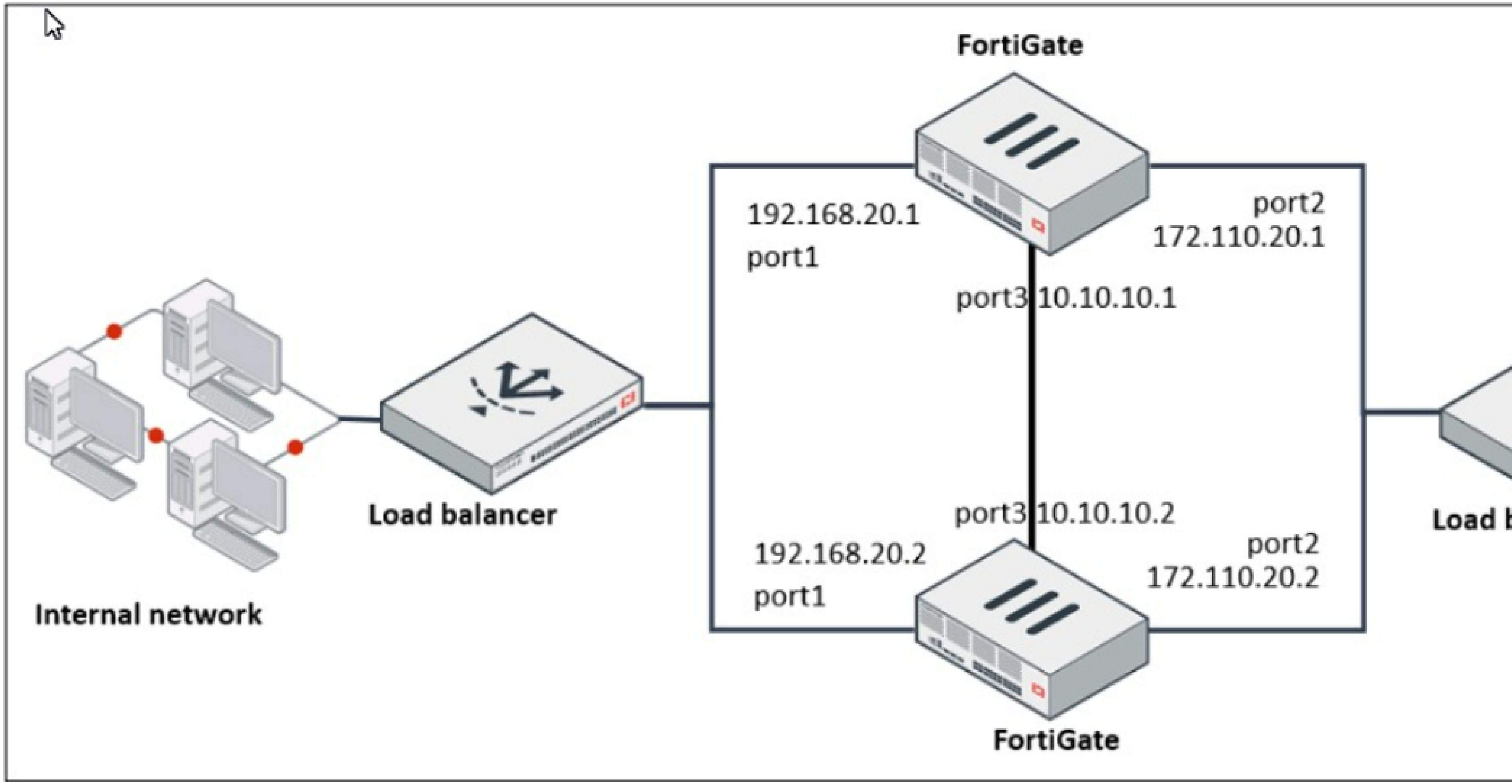
Explanation:

For a custom signature to be valid and savable on a FortiGate device, it must include certain mandatory fields. Severity is used to specify the level of threat that the signature represents, and attack_id is a unique identifier for the signature. Without these, the signature would not be complete and could not be correctly utilized by the FortiGate's Intrusion Prevention System (IPS).

Question 4

Question Type: **MultipleChoice**

Refer to the exhibit, which shows a network diagram.



Which protocol should you use to configure the FortiGate cluster?

Options:

A- FGCP in active-passive mode

B- OFGSP

C- VRRP

D- FGCP in active-active mode

Answer:

A

Explanation:

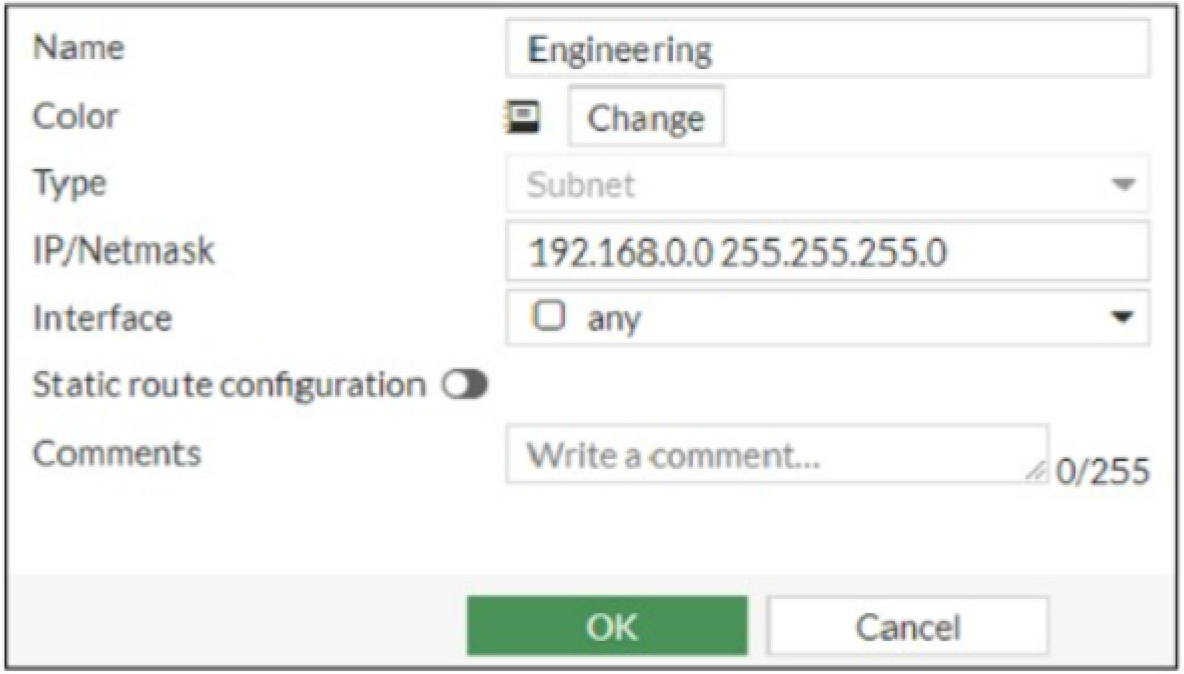
Given the network diagram and the presence of two FortiGate devices, the Fortinet Gate Clustering Protocol (FGCP) in active-passive mode is the most appropriate for setting up a FortiGate cluster. FGCP supports high availability configurations and is designed to allow one FortiGate to seamlessly take over if the other fails, providing continuous network availability. This is supported by Fortinet documentation for high availability configurations using FGCP.

Question 5

Question Type: MultipleChoice

Refer to the exhibits, which show the configurations of two address objects from the same FortiGate.

Engineering address object



Name: Engineering

Color

Type: Subnet

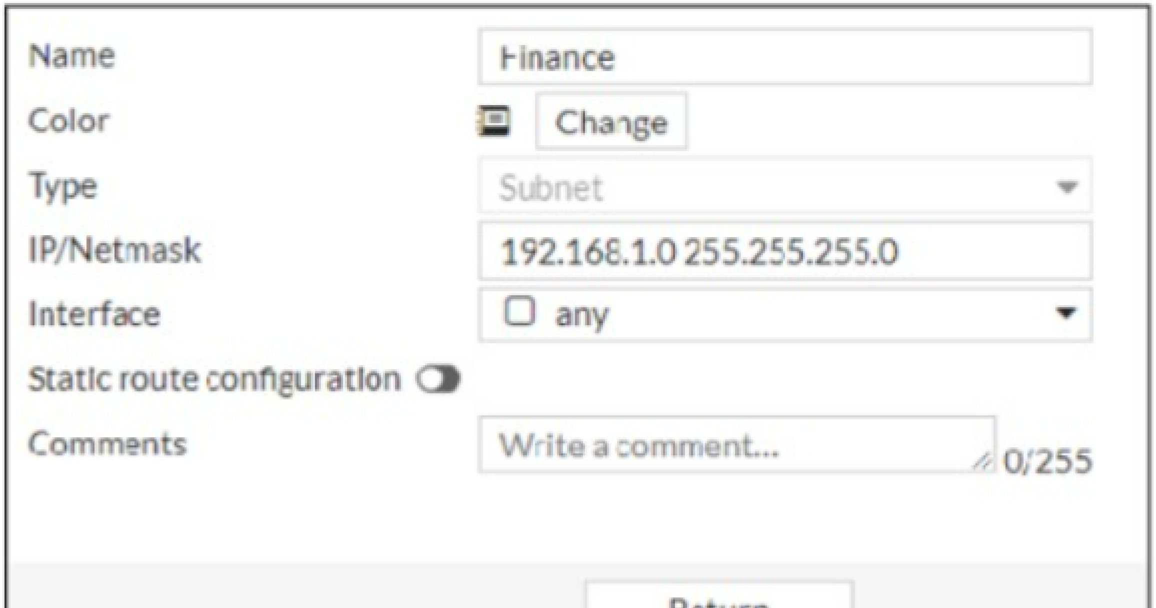
IP/Netmask: 192.168.0.0 255.255.255.0

Interface: □ any

Static route configuration

Comments: Write a comment... 0/255

Finance address object



Name: Finance

Color

Type: Subnet

IP/Netmask: 192.168.1.0 255.255.255.0

Interface: □ any

Static route configuration

Comments: Write a comment... 0/255

Why can you modify the Engineering address object, but not the Finance address object?

Options:

A- You have read-only access.

B- FortiGate joined the Security Fabric and the Finance address object was configured on the root FortiGate.

C- FortiGate is registered on FortiManager.

D- Another user is editing the Finance address object in workspace mode.

Answer:

B

Explanation:

The inability to modify the Finance address object while being able to modify the Engineering address object suggests that the Finance object is being managed by a higher authority in the Security Fabric, likely the root FortiGate. When a FortiGate is part of a Security Fabric, address objects and other configurations may be managed centrally. This aligns with the Fortinet FortiGate documentation on Security Fabric and central management of address objects.

Question 6

Question Type: MultipleChoice

Which two statements about the neighbor-group command are true? (Choose two.)

Options:

A- You can configure it on the GUI.

B- It applies common settings in an OSPF area.

C- It is combined with the neighbor-range parameter.

D- You can apply it in Internal BGP (IBGP) and External BGP (EBGP).

Answer:

B, D

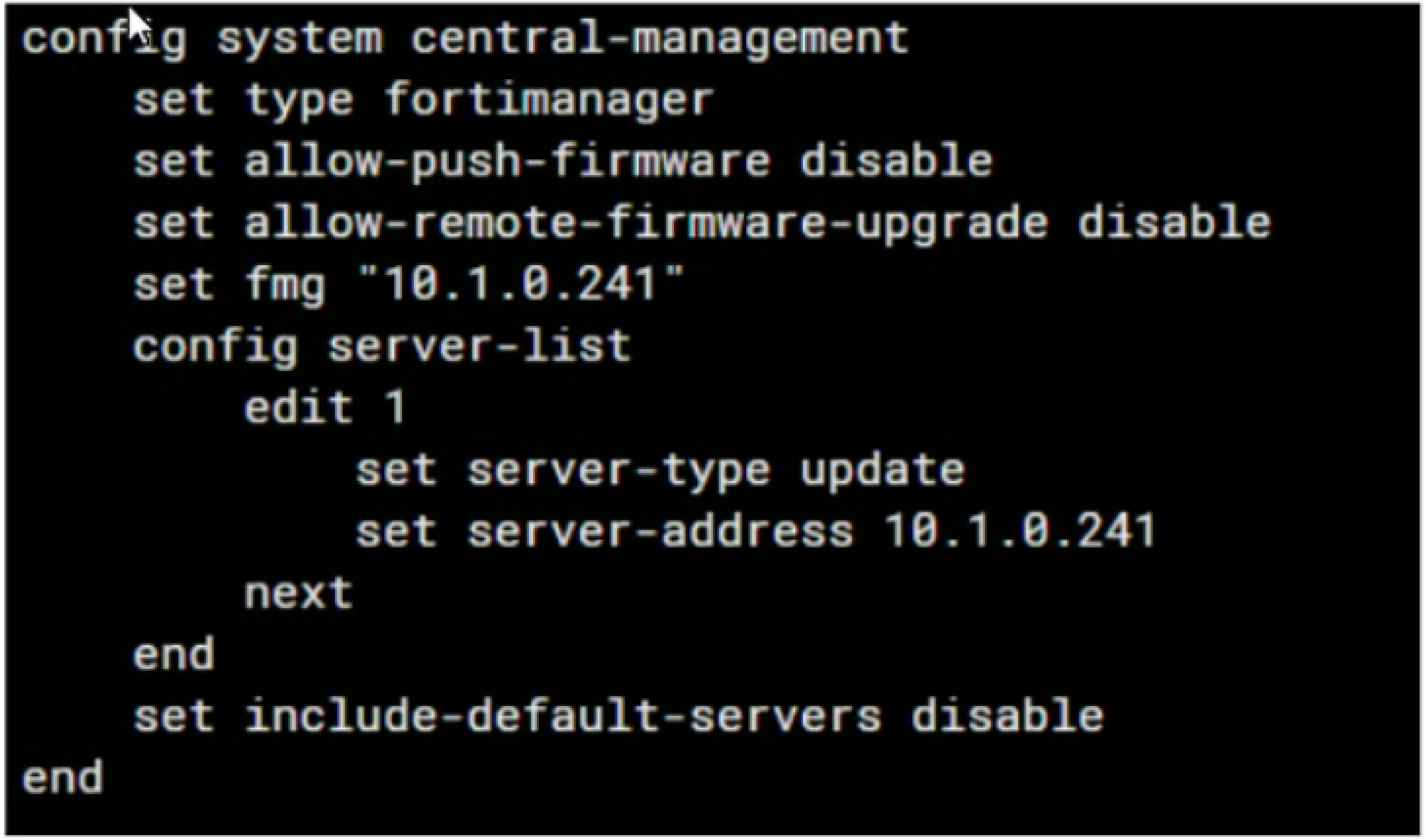
Explanation:

The neighbor-group command in FortiOS allows for the application of common settings to a group of neighbors in OSPF, and can also be used to simplify configuration by applying common settings to both IBGP and EBGP neighbors. This grouping functionality is a part of the FortiOS CLI and is documented in the Fortinet CLI reference.

Question 7

Question Type: **MultipleChoice**

Refer to the exhibit, which shows config system central-management information.



```
config system central-management
    set type fortimanager
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
    set fmg "10.1.0.241"
    config server-list
        edit 1
            set server-type update
            set server-address 10.1.0.241
        next
    end
    set include-default-servers disable
end
```

Which setting must you configure for the web filtering feature to function?

Options:

A- Add server. fortiguard. net to the server list.

B- Configure securewf.fortiguard. net on the default servers.

C- Set update-server-location to automatic.

D- Configure server-type with the rating option.

Answer:

D

Explanation:

For the web filtering feature to function effectively, the FortiGate device needs to have a server configured for rating services. The rating option in the server-type setting specifies that the server is used for URL rating lookup, which is essential for web filtering. The displayed configuration does not list any FortiGuard web filtering servers, which would be necessary for web filtering. The setting set include-default-servers disable indicates that the default FortiGuard servers are not being used, and hence, a specific server for web filtering (like securewf.fortiguard.net) needs to be configured.

Question 8

Question Type: MultipleChoice

Which two statements about the BFD parameter in BGP are true? (Choose two.)

Options:

A- It allows failure detection in less than one second.

B- The two routers must be connected to the same subnet.

C- It is supported for neighbors over multiple hops.

D- It detects only two-way failures.

Answer:

A, C

Explanation:

Bidirectional Forwarding Detection (BFD) is a rapid protocol for detecting failures in the forwarding path between two adjacent routers, including interfaces, data links, and forwarding planes. BFD is designed to detect forwarding path failures in a very short amount of time, often less than one second, which is significantly faster than traditional failure detection mechanisms like hold-down timers in routing protocols.

Fortinet supports BFD for BGP, and it can be used over multiple hops, which allows the detection of failures even if the BGP peers are not directly connected. This functionality enhances the ability to maintain stable BGP sessions over a wider network topology and is documented in Fortinet's guides.

Question 9

Question Type: **MultipleChoice**

Which two statements about IKE version 2 fragmentation are true? (Choose two.)

Options:

A- Only some IKE version 2 packets are considered fragmentable.

B- The reassembly timeout default value is 30 seconds.

C- It is performed at the IP layer.

D- The maximum number of IKE version 2 fragments is 128.

Answer:

A, D

Explanation:

In IKE version 2, not all packets are fragmentable. Only certain messages within the IKE negotiation process can be fragmented. Additionally, there is a limit to the number of fragments that IKE version 2 can handle, which is 128. This is specified in the Fortinet documentation and ensures that the IKE negotiation process can proceed even in networks that have issues with large packets. The reassembly timeout and the layer at which fragmentation occurs are not specified in this context within Fortinet documentation.

Question 10

Question Type: MultipleChoice

You want to improve reliability over a lossy IPSec tunnel.

Which combination of IPSec phase 1 parameters should you configure?

Options:

A- fec-ingress and fec-egress

B- Odpd and dpd-retryinterval

C- fragmentation and fragmentation-mtu

D- keepalive and keylive

Answer:

C

Explanation:

For improving reliability over a lossy IPSec tunnel, the fragmentation and fragmentation-mtu parameters should be configured. In scenarios where there might be issues with packet size or an unreliable network, setting the IPsec phase 1 to allow for fragmentation will enable large packets to be broken down, preventing them from being dropped due to size or poor network quality. The fragmentation-mtu specifies the size of the fragments. This is aligned with Fortinet's recommendations for handling IPsec VPN over networks with potential packet loss or size limitations.

Question 11

Question Type: **MultipleChoice**

Which two statements about ADVPN are true? (Choose two.)

Options:

A- You must disable add-route in the hub.

B- AllFortiGate devices must be in the same autonomous system (AS).

C- The hub adds routes based on IKE negotiations.

D- You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0.

Answer:

C, D

Explanation:

C) The hub adds routes based on IKE negotiations: This is part of the ADVPN functionality where the hub learns about the networks behind the spokes and can add routes dynamically based on the IKE negotiations with the spokes.

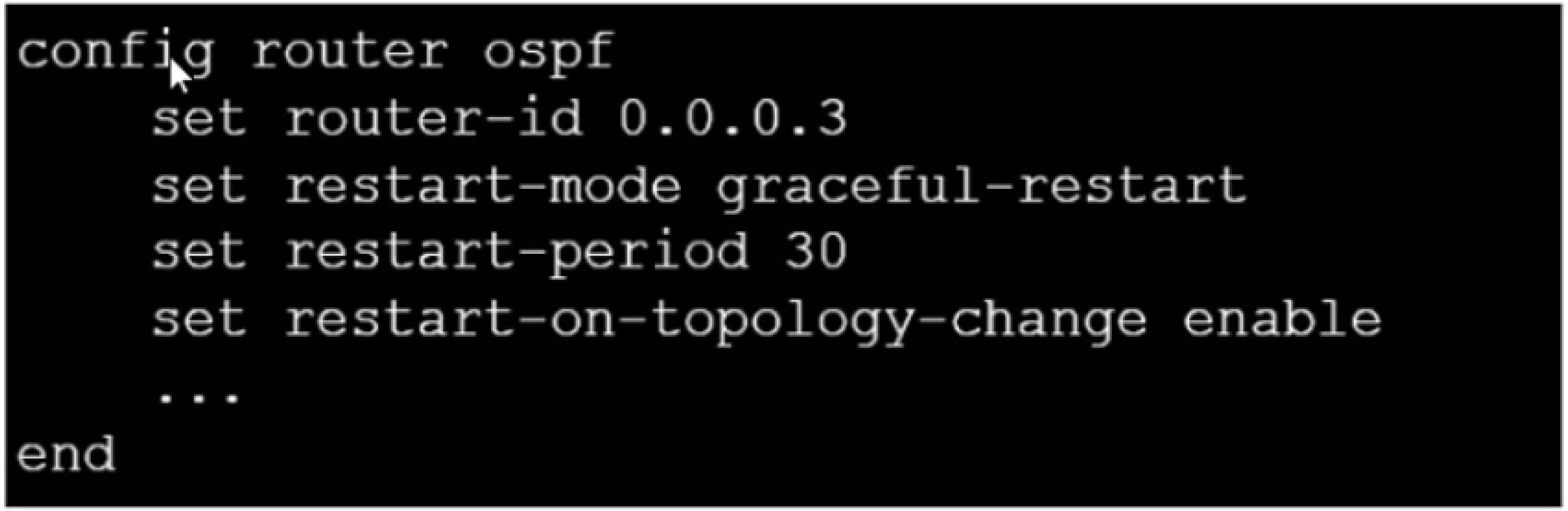
D) You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0: This wildcard setting in the phase 2 selectors allows any-to-any tunnel establishment, which is necessary for the dynamic creation of spoke-to-spoke tunnels.

These configurations are outlined in Fortinet's documentation for setting up ADVPN, where the hub's role in route control and the use of wildcard selectors for phase 2 are emphasized to enable dynamic tunneling between spokes.

Question 12

Question Type: MultipleChoice

Refer to the exhibit, which contains a partial OSPF configuration.



```
config router ospf
    set router-id 0.0.0.3
    set restart-mode graceful-restart
    set restart-period 30
    set restart-on-topology-change enable
    ...
end
```

What can you conclude from this output?

Options:

A- Neighbors maintain communication with the restarting router.

B- The router sends grace LSAs before it restarts.

C- FortiGate restarts if the topology changes.

D- The restarting router sends gratuitous ARP for 30 seconds.

Answer:

B

Explanation:

From the partial OSPF (Open Shortest Path First) configuration output:

B) The router sends grace LSAs before it restarts: This is implied by the command 'set restart-mode graceful-restart'. When OSPF is configured with graceful restart, the router sends grace LSAs (Link State Advertisements) to inform its neighbors that it is restarting, allowing for a seamless transition without recalculating routes.

Fortinet documentation on OSPF configuration clearly states that enabling graceful restart mode allows the router to maintain its adjacencies and routes during a brief restart period.