

# Fortinet

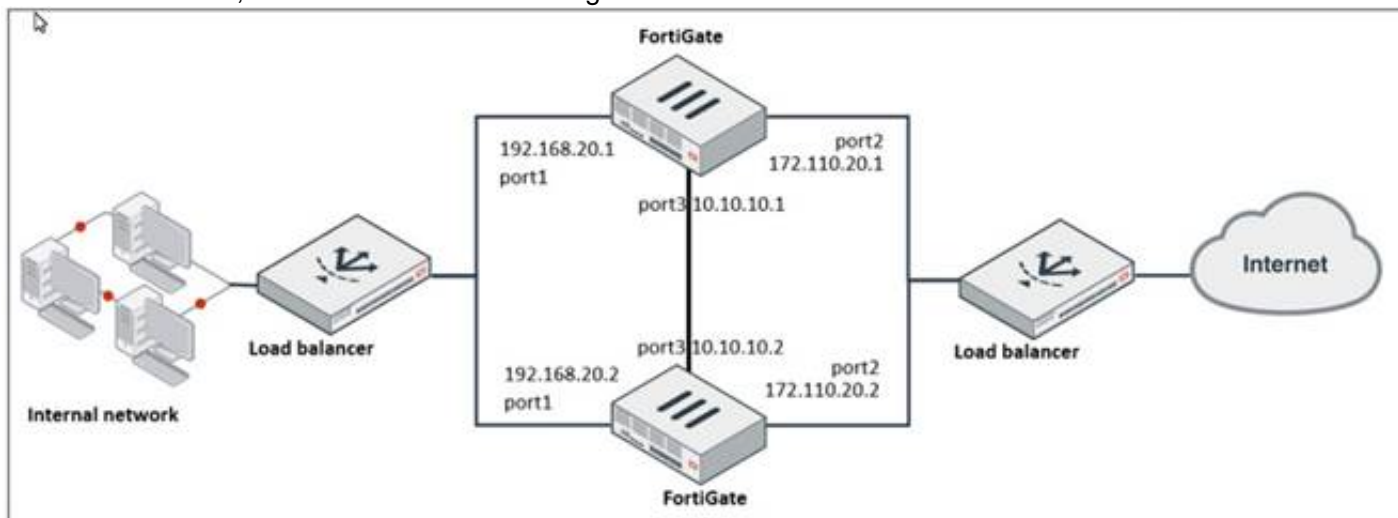
## Exam Questions NSE7\_EFW-7.2

Fortinet NSE 7 - Enterprise Firewall 7.2



### NEW QUESTION 1

Refer to the exhibit, which shows a network diagram.



Which protocol should you use to configure the FortiGate cluster?

- 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.

### NEW QUESTION 2

Which two statements about bfd are true? (Choose two)

- A. It can support neighbor only over the next hop in BGP
- B. You can disable it at the protocol level
- C. It works for OSPF and BGP
- D. You must configure n globally only

**Answer: BC**

#### Explanation:

BFD (Bidirectional Forwarding Detection) is a protocol that can quickly detect failures in the forwarding path between two adjacent devices. You can disable BFD at the protocol level by using the "set bfd disable" command under the OSPF or BGP configuration. BFD works for both OSPF and BGP protocols, as well as static routes and SD-WAN rules. References := BFD | FortiGate / FortiOS 7.2.0 - Fortinet Document Library, section "BFD".

### NEW QUESTION 3

Refer to the exhibit, which shows a custom signature.



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

- A. Add severity.
- B. Add attack\_id.
- C. Ensure that the header syntax is F-SBID.
- D. Start options with --.

**Answer: AB**

#### 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).

### NEW QUESTION 4

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

- 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).

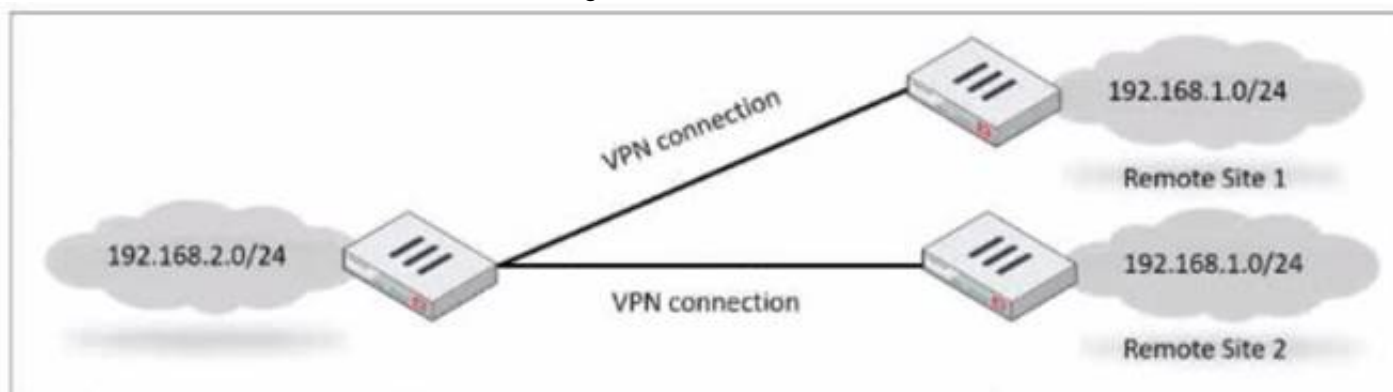
**Answer:** BD

**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.

**NEW QUESTION 5**

Refer to the exhibit, which shows a network diagram.



Which IPsec phase 2 configuration should you implement so that only one remote site is connected at any time?

- A. Set route-overlap to allow.
- B. Set single-source to enable
- C. Set route-overlap to either use—new or use-old
- D. Set net-device to enable

**Answer:** C

**Explanation:**

To ensure that only one remote site is connected at any given time in an IPsec VPN scenario, you should use route-overlap with the option to either use-new or use-old. This setting dictates which routes are preferred and how overlaps in routes are handled, allowing for one connection to take precedence over the other (C).

References:

? FortiOS Handbook - IPsec VPN

**NEW QUESTION 6**

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

- 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:** AC

**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.


**NEW QUESTION 7**

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

### Engineering address object

Name	Engineering
Color	 <input type="button" value="Change"/>
Type	Subnet
IP/Netmask	192.168.0.0 255.255.255.0
Interface	<input type="checkbox"/> any
Static route configuration	<input type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### Finance address object

Name	Finance
Color	 <input type="button" value="Change"/>
Type	Subnet
IP/Netmask	192.168.1.0 255.255.255.0
Interface	<input type="checkbox"/> any
Static route configuration	<input type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
<input type="button" value="Return"/>	

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

- 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.

### NEW QUESTION 8

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.

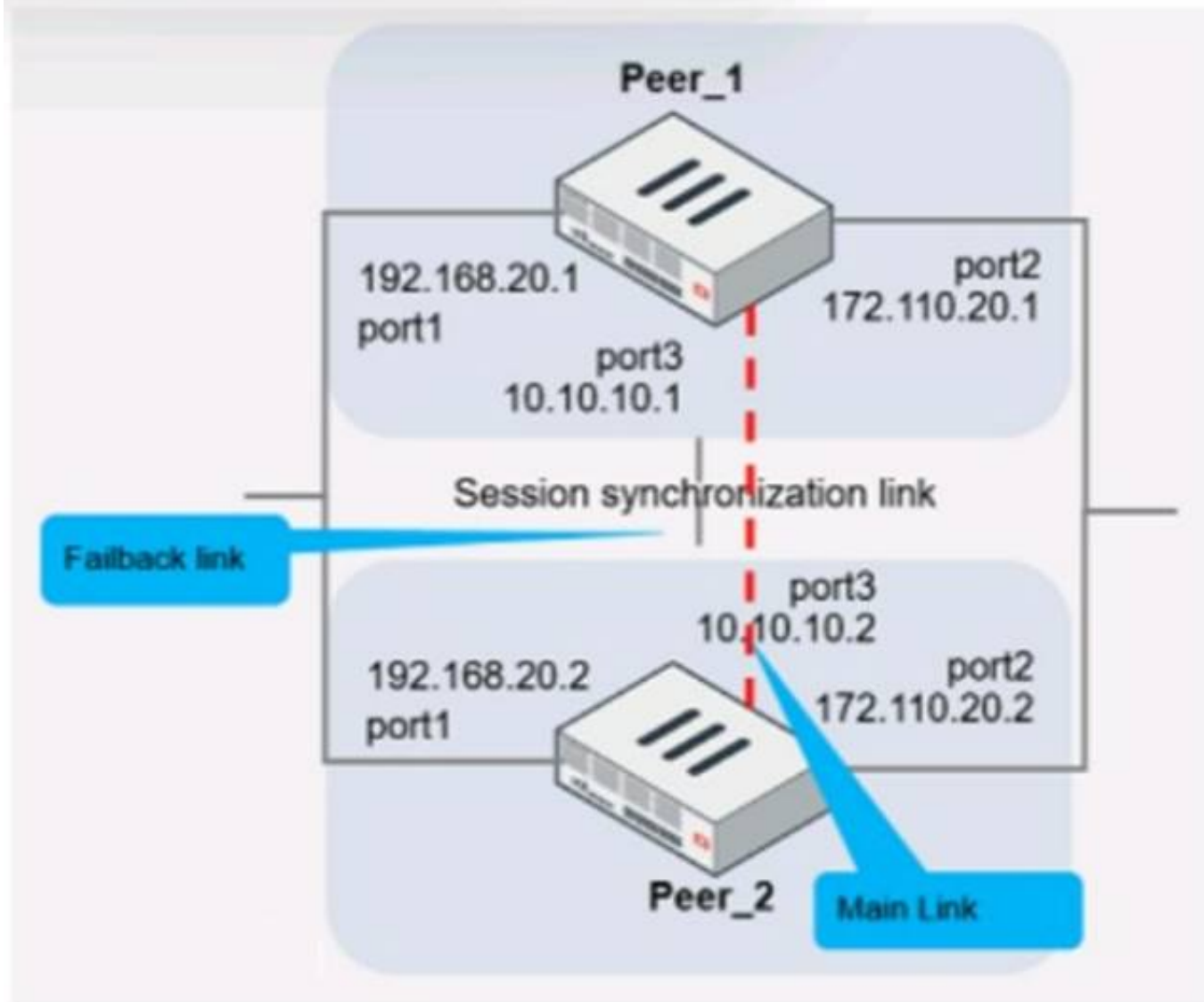
**Answer: C**

**Explanation:**

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

**NEW QUESTION 9**

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 <interface> command.  
 What is the primary reason to configure the main link?

- 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.

**NEW QUESTION 10**

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 are disabled
- C. Only NPs are disabled
- D. NPs and CPs are disabled

**Answer: D**

**Explanation:**

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

**NEW QUESTION 10**

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

- A. Phase 1 includes main mode
- B. It supports the extensible authentication protocol (EAP)
- C. It supports the XAuth protocol.
- D. It exchanges a minimum of four messages to establish a secure tunnel

**Answer: BD**

**Explanation:**

IKE version 2 supports the extensible authentication protocol (EAP), which allows for more flexible and secure authentication methods<sup>1</sup>. IKE version 2 also exchanges a minimum of four messages to establish a secure tunnel, which is more efficient than IKE version 1<sup>2</sup>. References: <sup>1</sup> = IKE settings | FortiClient 7.2.2 - Fortinet

Documentation, Technical Tip: How to configure IKE version 1 or 2 ... - Fortinet Community

**NEW QUESTION 13**

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/Down   State/PfxRcd
10.125.0.60    4  65060    1698    1756     103    0    0    03:02:49      1
10.127.0.75    4  65075    2206    2250     102    0    0    02:45:55      1
100.64.3.1     4  65501     101     115       0    0    0      never      Active

Total number of neighbors 3
```

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

- 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: AB**

**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.

#### NEW QUESTION 16

Which configuration can be used to reduce the number of BGP sessions in on IBGP network?

- A. Route-reflector-peer enable
- B. Route-reflector-client enable
- C. Route-reflector enable
- D. Route-reflector-server enable

**Answer: B**

#### Explanation:

To reduce the number of BGP sessions in an IBGP network, you can use a route reflector, which acts as a focal point for IBGP sessions and readvertises the prefixes to all other peers. To configure a route reflector, you need to enable the route-reflector- client option on the neighbor-group settings of the hub device. This will make the hub device act as a route reflector server and the other devices as route reflector clients. References := Route exchange | FortiGate / FortiOS 7.2.0 - Fortinet Documentation

#### NEW QUESTION 18

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

- 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: CD**

#### 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.

#### NEW QUESTION 20

Which statement about network processor (NP) offloading is true?

- A. For TCP traffic FortiGate CPU offloads the first packets of SYN/ACK and ACK of the three-way handshake to NP
- B. The NP provides IPS signature matching
- C. You can disable the NP for each firewall policy using the command np-acceleration st to loose.
- D. The NP checks the session key or IPSec SA

**Answer: B**

#### Explanation:

Network processors (NPs) are specialized hardware within FortiGate devices that accelerate certain security functions. One of the primary functions of NPs is to provide IPS signature matching (B), allowing for high-speed inspection of traffic against a database of known threat signatures.

#### NEW QUESTION 24

Exhibit.

```
config system central-management
  set type fortimanager
  set fmg "10.0.1.242"
  config server-list
    edit 1
      set server-type rating
      set addr-type ipv4
      set server-address 10.0.1.240
    next
    edit 2
      set server-type update
      set addr-type ipv4
      set server-address 10.0.1.243
    next
    edit 3
      set server-type rating
      set addr-type ipv4
      set server-address 10.0.1.244
    next
  end
  set include-default-servers enable
end
```

Refer to exhibit, which shows a central management configuration  
 Which server will FortiGate choose for web filter rating requests if 10.0.1.240 is experiencing an outage?

- A. Public FortiGuard servers
- B. 10.0.1.242
- C. 10.0.1.244
- D. 10.0.1.243

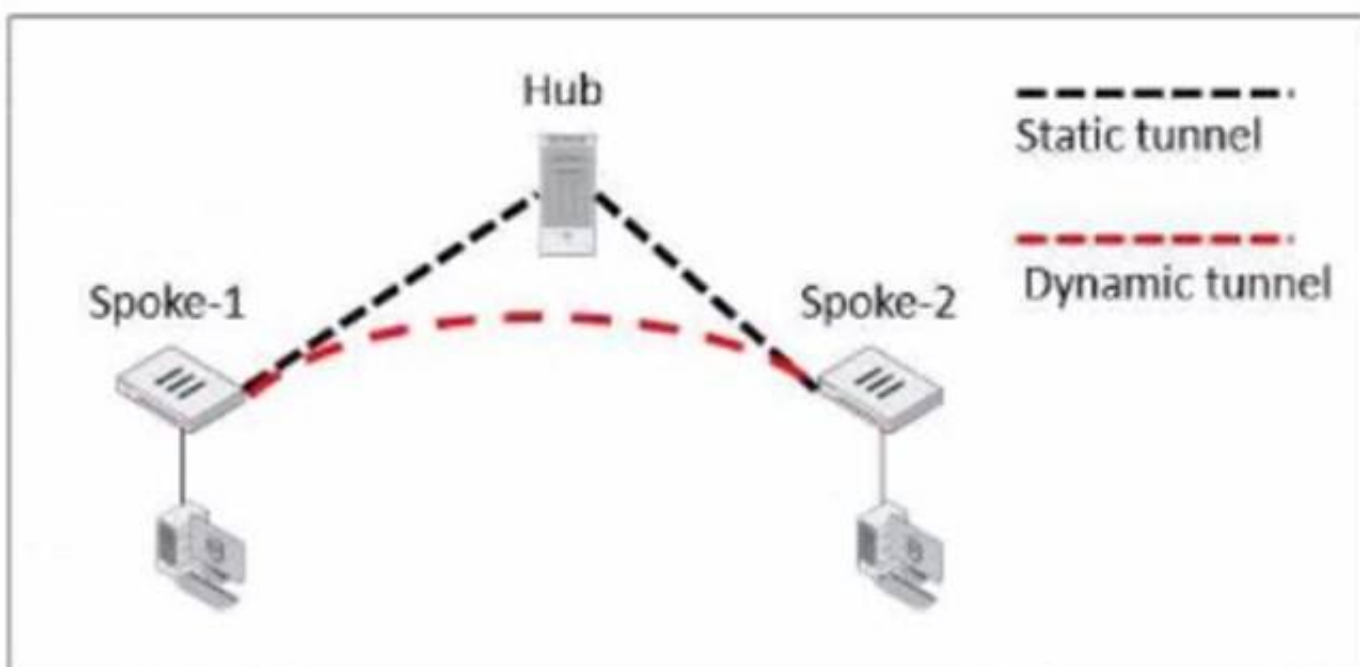
**Answer: C**

**Explanation:**

In the event of an outage at 10.0.1.240, the FortiGate will choose the next server in the sequence for web filter rating requests, which is 10.0.1.244 according to the configuration shown in the exhibit. This is because the server list is ordered by priority, and the server with the lowest priority number is chosen first. If that server is unavailable, the next server with the next lowest priority number is chosen, and so on. The public FortiGuard servers are only used if the include-default-servers option is enabled and all the custom servers are unavailable. References := Fortinet Enterprise Firewall Study Guide for FortiOS 7.2, page 132.

**NEW QUESTION 27**

Exhibit.



Refer to the exhibit, which shows an ADVPN network.  
 The client behind Spoke-1 generates traffic to the device located behind Spoke-2. Which first message does the hub send to Spoke-1 to bring up the dynamic tunnel?

- A. Shortcut query
- B. Shortcut reply
- C. Shortcut offer
- D. Shortcut forward



Answer: A

Explanation:

In an ADVPN scenario, when traffic is initiated from a client behind one spoke to another spoke, the hub sends a shortcut query to the initiating spoke. This query is used to determine if there is a more direct path for the traffic, which can then trigger the establishment of a dynamic tunnel between the spokes.

NEW QUESTION 31

Refer to the exhibit, which contains a partial BGP combination.

```
config router bgp
  set as 65200
  set router-id 172.16.1.254
  config neighbor
    edit 100.64.1.254
      set remote-as 65100
    next
  end
end
```

You want to configure a loopback as the OGP source.  
Which two parameters must you set in the BGP configuration? (Choose two)

- A. ebgp-enforce-multihop
- B. recursive-next-hop
- C. ibgp-enfoce-multihop
- D. update-source

Answer: AD

Explanation:

To configure a loopback as the BGP source, you need to set the “ebgp- enforce-multihop” and “update-source” parameters in the BGP configuration. The “ebgp- enforce-multihop” allows EBGP connections to neighbor routers that are not directly connected, while “update-source” specifies the IP address that should be used for the BGP session1. References := BGP on loopback, Loopback interface, Technical Tip: Configuring EBGP Multihop Load-Balancing, Technical Tip: BGP routes are not installed in routing table with loopback as update source

NEW QUESTION 32

Refer to the exhibit, which shows a routing table.

Network #	Gateway IP #	Interfaces #	Distance #	Type #
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

Answer: BC

Explanation:

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

NEW QUESTION 33

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?

- A. Add serve
- B. fortiguar
- C. net to the server list.
- D. Configure securewf.fortiguar
- E. net on the default servers.
- F. Set update-server-location to automatic.
- G. 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.

**NEW QUESTION 38**

Exhibit.

Script Name	Static Route
Comments	<div>0/255</div> <div>0/255</div>
Type	CLI Script
Run script on	Remote FortiGate Directly (...)
Script details	<pre># conf rout stat #   edit 0 #       set gateway 10.20.121.2 #       set priority 20 #       set device "wan1" #   next # end</pre>

Refer to the exhibit, which contains a CLI script configuration on fortiManager. An administrator configured the CLI script on FortiManager rut the script tailed to apply any changes to the managed device after being executed.

What are two reasons why the script did not make any changes to the managed device? (Choose two)

- A. The commands that start with the # sign did not run.
- B. Incomplete commands can cause CLI scripts to fail.
- C. Static routes can be added using only TCI scripts.

D. CLI scripts must start with #!.

**Answer:** AB

**Explanation:**

The commands that start with the # sign did not run because they are treated as comments in the CLI script. Incomplete commands can cause CLI scripts to fail because they are not recognized by the FortiGate device. The other options are incorrect because static routes can be added using CLI or GUI, and CLI scripts do not need to start with #!. References := Configuring custom scripts | FortiManager 7.2.0 - Fortinet Documentation, section "CLI script syntax".

**NEW QUESTION 40**

You configured 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 FortiGate has fabric-object-unification set to local
- D. The downstream FortiGate has configuration-sync set to local

**Answer:** AC

**Explanation:**

? 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

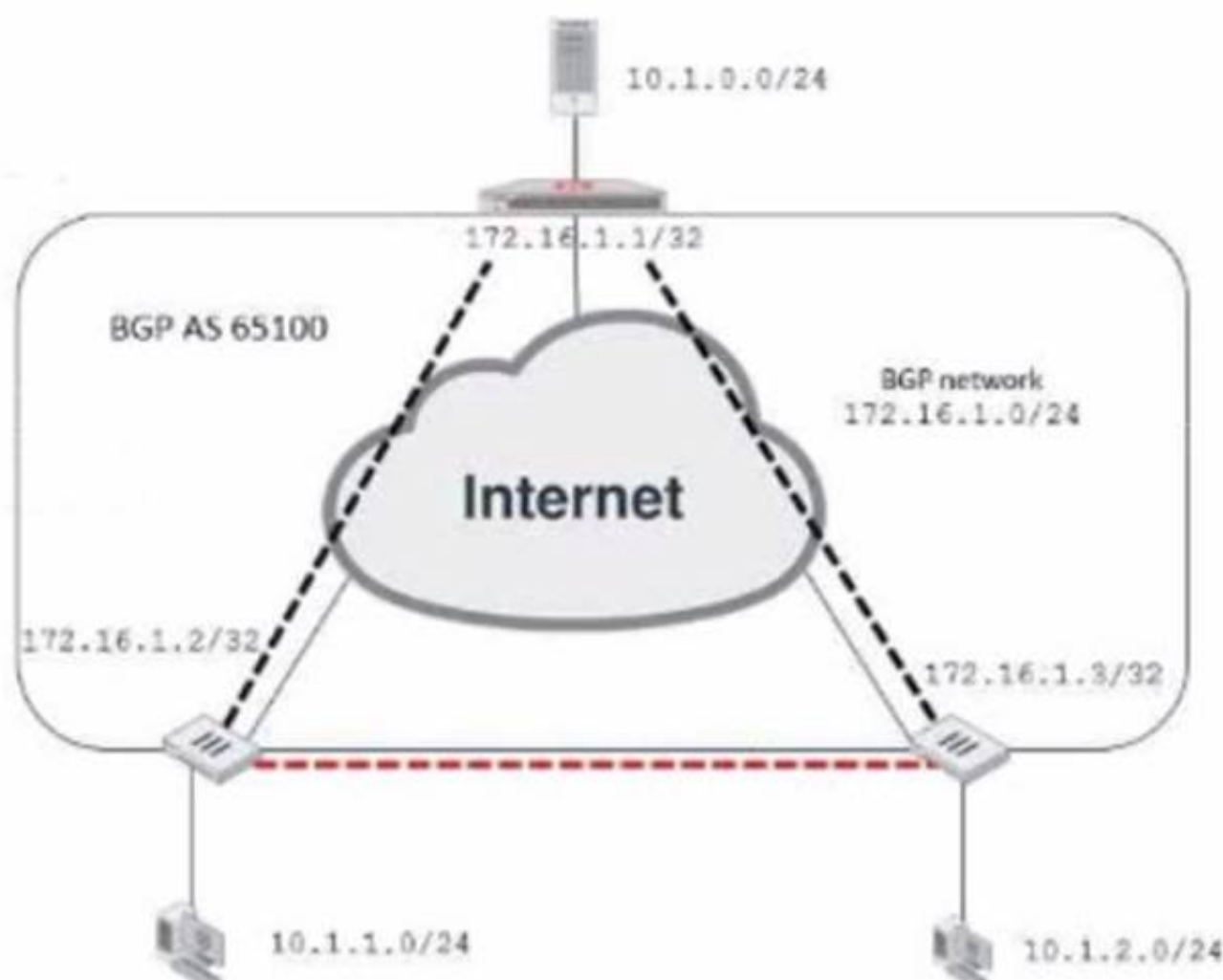
? 4: Configuration synchronization7

? : Security Fabric - Fortinet Documentation

**NEW QUESTION 43**

Exhibit.

**Network diagram**



## Partial BGP configuration

```

Hub # show router bgp
config router bgp
  set as 65100
  set router-id 172.16.1.1
  config neighbor-group
    edit "advpn"
      set remote-as 65100
      ...
    next
  end
  ...
end

```

Refer to the exhibit, which contains an ADVPN network diagram and a partial BGP configuration. Which two parameters should you configure in config neighbor range? (Choose two.)

- A. set prefix 172.16.1.0 255.255.255.0
- B. set route reflector-client enable
- C. set neighbor-group advpn
- D. set prefix 10.1.0 255.255.255.0

**Answer:** AC

### Explanation:

In the ADVPN configuration for BGP, you should specify the prefix that the neighbors can advertise. Option A is correct as you would configure the BGP network prefix that should be advertised to the neighbors, which matches the BGP network in the diagram. Option C is also correct since you should reference the neighbor group configured for the ADVPN setup within the BGP configuration.

## NEW QUESTION 44

An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device. What can the administrator do to fix this problem?

- A. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports
- B. Configure set link-failed-signal enable under config system ha on both cluster members
- C. Configure remote link monitoring to detect an issue in the forwarding path
- D. Configure set send-garp-on-failover enables under config system ha on both cluster members

**Answer:** B

### Explanation:

Virtual MAC Address and Failover

- The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port.
- Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces):

```
#Config system ha
```

```
set link-failed-signal enable end
```

- This simulates a link failure that clears the related entries from MAC table of the switches.

## NEW QUESTION 46

Exhibit.



```
# diagnose webfilter fortiguard cache dump

Saving to file [/tmp/urcCache.txt]
Cache Contents:
-----
Cache Mode:    TTL
Cache DB Ver:  23.6106

Domain |IP      DB Ver  T URL
34000000|34000000 23.6106 P Bhttp://training.fortinet.com/
25000000|25000000 23.6106 E Bhttps://twitter.com/...

# get webfilter categories
...
g07 General Interest - Business:
  31 Finance and Banking
...
  51 Government and Legal Organizations
  52 Information Technology
```

Refer to the exhibit, which shows the output from the webfilter fortiguard cache dump and webfilter categories commands. Using the output, how can an administrator determine the category of the training.fortinet.com website?

- A. The administrator must convert the first three digits of the IP hex value to binary
- B. The administrator can look up the hex value of 34 in the second command output.
- C. The administrator must add both the Pima in and lphex values of 34 to get the category number
- D. The administrator must convert the first two digits of the Domain hex value to a decimal value

**Answer: B**

**Explanation:**

? Option B is correct because the administrator can determine the category of the training.fortinet.com website by looking up the hex value of 34 in the second command output. This is because the first command output shows that the domain and the IP of the website are both in category (Hex) 34, which corresponds to Information Technology in the second command output<sup>1</sup>.

? Option A is incorrect because the administrator does not need to convert the first three digits of the IP hex value to binary. The IP hex value is already in the same format as the category hex value, so the administrator can simply compare them without any conversion<sup>2</sup>.

? Option C is incorrect because the administrator does not need to add both the

Pima in and lphex values of 34 to get the category number. The Pima in and lphex values are not related to the category number, but to the cache TTL and the database version respectively<sup>3</sup>.

? Option D is incorrect because the administrator does not need to convert the first

two digits of the Domain hex value to a decimal value. The Domain hex value is already in the same format as the category hex value, so the administrator can simply compare them without any conversion<sup>2</sup>. References: =

? 1: Technical Tip: Verify the webfilter cache content<sup>4</sup>

? 2: Hexadecimal to Decimal Converter<sup>5</sup>

? 3: FortiGate - Fortinet Community<sup>6</sup>

? : Web filter | FortiGate / FortiOS 7.2.0 - Fortinet Documentation<sup>7</sup>

**NEW QUESTION 49**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### NSE7\_EFW-7.2 Practice Exam Features:

- \* NSE7\_EFW-7.2 Questions and Answers Updated Frequently
- \* NSE7\_EFW-7.2 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE7\_EFW-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE7\_EFW-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE7\\_EFW-7.2 Practice Test Here](#)**