

# Fortinet

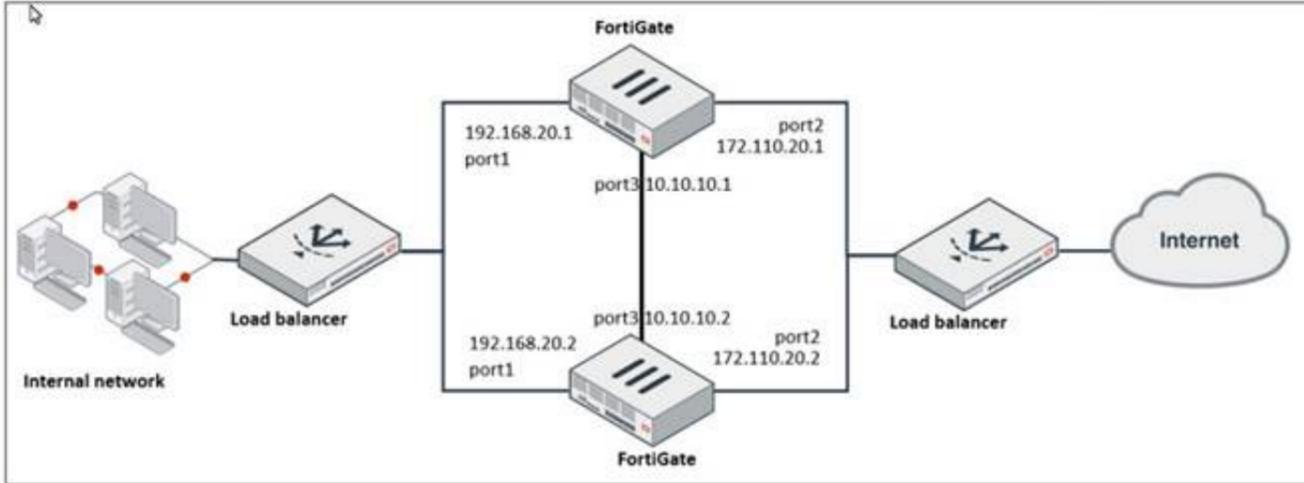
## Exam Questions NSE7\_EFW-7.2

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**

Winch two statements about ADVPN are true? (Choose two)

- A. auto-discovery receiver must be set to enable on the Spokes.
- B. Spoke to-spoke traffic never goes through the hub
- C. It supports NAI for on-demand tunnels
- D. Routing is configured by enabling add-advpn-route

**Answer: AC**

**Explanation:**

ADVPN (Auto Discovery VPN) is a feature that allows to dynamically establish direct tunnels (called shortcuts) between the spokes of a traditional Hub and Spoke architecture. The auto-discovery receiver must be set to enable on the spokes to allow them to receive NHRP messages from the hub and other spokes. NHRP (Next Hop Resolution Protocol) is used for on-demand tunnels, which are established when there is traffic between spokes. Routing is configured by enabling add-nhrp-route, not add-advpn- route. References := ADVPN | FortiGate / FortiOS 7.2.0 | Fortinet Document Library, Technical Tip: Fortinet Auto Discovery VPN (ADVPN)

**NEW QUESTION 3**

Which two statements about the Security fabric are true? (Choose two.)

- A. FortiGate uses the FortiTelemetry protocol to communicate with FortiAnalyzer.
- B. Only the root FortiGate sends logs to FortiAnalyzer
- C. Only FortiGate devices with configuration-sync receive and synchronize global CMDB objects that the toot FortiGate sends
- D. Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer

**Answer: BC**

**Explanation:**

In the Security Fabric, only the root FortiGate sends logs to FortiAnalyzer (B). Additionally, only FortiGate devices with configuration-sync enabled receive and synchronize global Central Management Database (CMDB) objects that the root FortiGate sends (C). FortiGate uses the FortiTelemetry protocol to communicate with other FortiGates, not FortiAnalyzer (A). The last option (D) is incorrect as all FortiGates can collect and forward network topology information to FortiAnalyzer. References: ? FortiOS Handbook - Security Fabric

**NEW QUESTION 4**

Refer to the exhibit, which contains information about an IPsec VPN tunnel.

```
FortiGate # diag vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=tunnel_0 ver=2 serial=1 100.64.3.1:0->100.64.1.1:0 tun_id=100.64.1.1 tun_id6=:100.64.1.1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc run_s
proxyid_num=1 child_num=0 refcnt=3 ilast=42949917 olast=42949917 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=off on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=tunnel_0_0 proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:0.0.0.0-255.255.255.255:0
SA: ref=3 options=30202 type=00 soft=0 mtu=1280 expire=1454/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 qat=192 rekey=0 hash_search_len=1
life: type=01 bytes=0/0 timeout=1768/1800
dec: spi=877d6590 esp=aes key=16 be308ec1fb05464205764424bc40a76d
ah=sha256 key=32 cc8894be3390983521a48b2e7a5c998e6b28a18a3ddd8e7bc7ecbe672dfe7cc5
enc: spi=63d0f38a esp=aes key=16 d8d3343af2fed4ddd958a022cd656b06
ah=sha256 key=32 264402ba8ad04a7e97732b52ec27c92ff86e0a97bb33e22887677336f1670c7d
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
npu_flag=00 npu_rgw=100.64.1.1 npu_lgwy=100.64.3.1 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

What two conclusions can you draw from the command output? (Choose two.)

- A. Dead peer detection is set to enable.
- B. The IKE version is 2.
- C. Both IPsec SAs are loaded on the kernel.
- D. Forward error correction in phase 2 is set to enable.

**Answer: BC**

**Explanation:**

From the command output shown in the exhibit:

\* B. The IKE version is 2: This can be deduced from the presence of 'ver=2' in the output, which indicates that IKEv2 is being used.

\* C. Both IPsec SAs are loaded on the kernel: This is indicated by the line 'npu flags=0x0/0', suggesting that no offload to NPU is occurring, and hence, both Security Associations are loaded onto the kernel for processing.

Fortinet documentation specifies that the version of IKE (Internet Key Exchange) used and the loading of IPsec Security Associations can be verified through the diagnostic commands related to VPN tunnels.

**NEW QUESTION 5**

You want to block access to the website ww.eicar.org using a custom IPS signature. Which custom IPS signature should you configure?

- A)

```
F-SBID( --name "eicar"; --protocol udp; --flow from_server; --pattern "eicar"; --context host;)
```
- B)

```
F-SBID( --name "detect_eicar"; --protocol udp; --service ssl; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)
```
- C)

```
F-SBID( --name "detect_eicar"; --protocol tcp; --service dns; --flow from_server; --pattern "eicar"; --no_case;)
```
- D)

```
F-SBID( --name "eicar"; --protocol tcp; --service HTTP; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

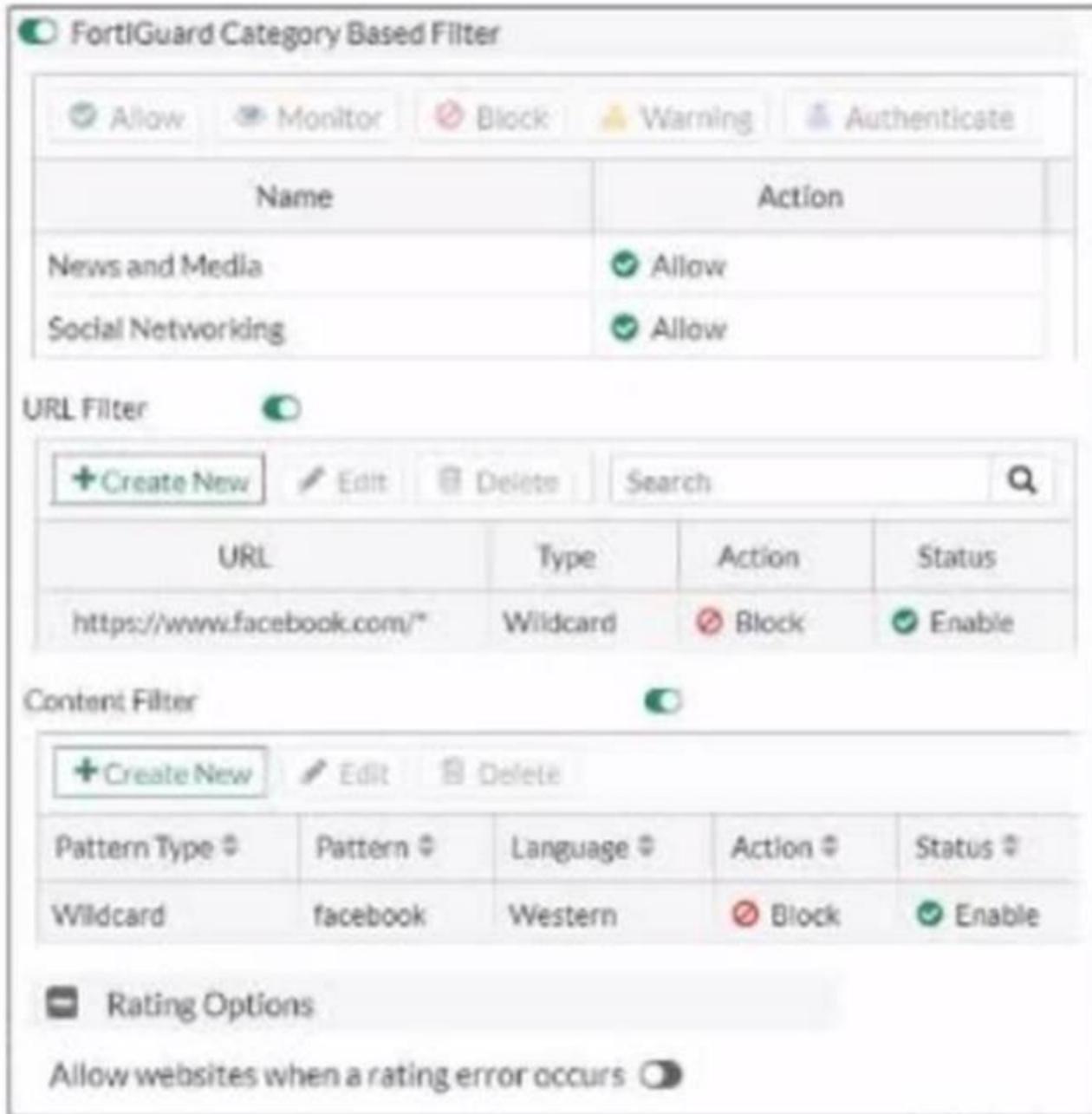
**Answer: D**

**Explanation:**

Option D is the correct answer because it specifically blocks access to the website "www.eicar.org" using TCP protocol and HTTP service, which are commonly used for web browsing. The other options either use the wrong protocol (UDP), the wrong service (DNS or SSL), or the wrong pattern ("eicar" instead of "www.eicar.org"). References := Configuring custom signatures | FortiGate / FortiOS 7.4.0 - Fortinet Document Library, section "Signature to block access to example.com".

**NEW QUESTION 6**

Exhibit.



Refer to the exhibit, which shows a partial web filter profile configuration. What can you conclude from this configuration about access to www.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 blocked if the local or the public FortiGuard server does not reply

**Answer: C**

**Explanation:**

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 section. 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

**NEW QUESTION 7**

Exhibit.

```
config vpn ipsec phase1-interface
edit tunnel
set type dynamic
set interface "port1"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256 aes256-sha256
set dpd on-idle
set add-route enable
set psksecret fortinet
next
end
```

Refer to the exhibit, which contains a partial VPN configuration. What can you conclude from this configuration?

- A. FortiGate creates separate virtual interfaces for each dial up client.
- B. The VPN should use the dynamic routing protocol to exchange routing information Through the tunnels.

- C. Dead peer detection is disabled.
- D. The routing table shows a single IPsec virtual interface.

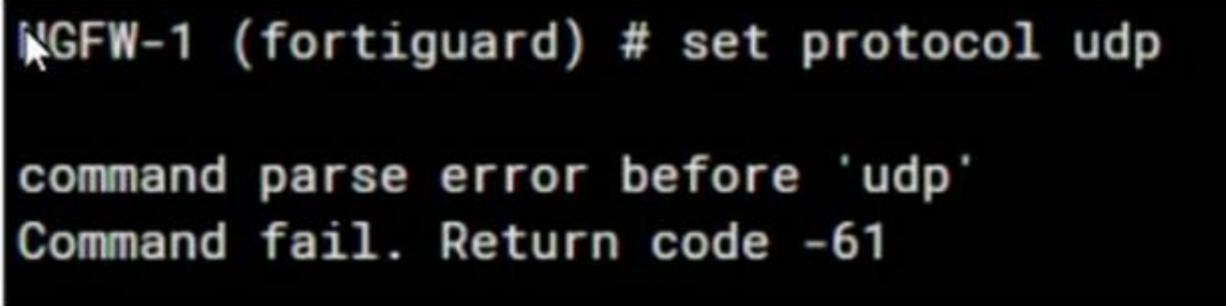
**Answer:** C

**Explanation:**

The configuration line "set dpd on-idle" indicates that dead peer detection (DPD) is set to trigger only when the tunnel is idle, not actively disabled. References: FortiGate IPsec VPN User Guide - Fortinet Document Library  
From the given VPN configuration, dead peer detection (DPD) is set to 'on-idle', indicating that DPD is enabled and will be used to detect if the other end of the VPN tunnel is still alive when no traffic is detected. Hence, option C is incorrect. The configuration shows the tunnel set to type 'dynamic', which does not create separate virtual interfaces for each dial-up client (A), and it is not specified that dynamic routing will be used (B). Since this is a phase 1 configuration snippet, the routing table aspect (D) cannot be concluded from this alone.

**NEW QUESTION 8**

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



```
FGFW-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.

**Answer:** D

**Explanation:**

The reason for the command failure when trying to set the protocol to UDP in the config system fortiguard is 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.

**NEW QUESTION 9**

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

Engineering address object

Name	Engineering
Color	 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	Write a comment... 0/255
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Finance address object

Name	Finance
Color	 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	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 10**

You want to configure faster failure detection for BGP

Which parameter should you enable on both connected FortiGate devices?

- A. Ebgp-enforce-multihop
- B. bfd
- C. Distribute-list-in
- D. Graceful-restart

**Answer: B**

**Explanation:**

BFD (Bidirectional Forwarding Detection) is a protocol that provides fast failure detection for BGP by sending periodic messages to verify the connectivity between two peers<sup>1</sup>. BFD can be enabled on both connected FortiGate devices by using the command set bfd enable under the BGP configuration<sup>2</sup>. References: =

Technical Tip :

FortiGate BFD implementation and examples ..., Configure BGP | FortiGate / FortiOS 7.0.2

- Fortinet Documentation

#### NEW QUESTION 10

Which ADVPN configuration must be configured using a script on FortiManager, when using VPN Manager to manage FortiGate VPN tunnels?

- A. Enable AD-VPN in IPsec phase 1
- B. Disable add-route on hub
- C. Configure IP addresses on IPsec virtual interfaces
- D. Set protected network to all

**Answer:** A

#### Explanation:

To enable AD-VPN, you need to edit an SD-WAN overlay template and enable the Auto-Discovery VPN toggle. This will automatically add the required settings to the IPsec template and the BGP template. You cannot enable AD-VPN directly in the IPsec phase 1 settings using VPN Manager. References := ADVPN | FortiManager 7.2.0 - Fortinet Documentation

#### NEW QUESTION 14

After enabling IPS you receive feedback about traffic being dropped. What could be the reason?

- A. Np-accel-mode is set to enable
- B. Traffic-submit is set to disable
- C. IPS is configured to monitor
- D. Fail-open is set to disable

**Answer:** D

#### Explanation:

Fail-open is a feature that allows traffic to pass through the IPS sensor without inspection when the sensor fails or is overloaded. If fail-open is set to disable, traffic will be dropped in such scenarios. References := IPS | FortiGate / FortiOS 7.2.3 - Fortinet Documentation  
When IPS (Intrusion Prevention System) is configured, if fail-open is set to disable, it means that if the IPS engine fails, traffic will not be allowed to pass through, which can result in traffic being dropped (D). This is in contrast to a fail-open setting, which would allow traffic to bypass the IPS engine if it is not operational.

#### NEW QUESTION 15

Which two statements about metadata variables are true? (Choose two.)

- A. You create them on FortiGate
- B. They apply only to non-firewall objects.
- C. The metadata format is \$<metadata\_variable\_name>.
- D. They can be used as variables in scripts

**Answer:** AD

#### Explanation:

Metadata variables in FortiGate are created to store metadata associated with different FortiGate features. These variables can be used in various configurations and scripts to dynamically replace the variable with its actual value during processing. A: You create metadata variables on FortiGate. They are used to store metadata for FortiGate features and can be called upon in different configurations. D: They can be used as variables in scripts. Metadata variables are utilized within the scripts to dynamically insert values as per the context when the script runs.

Fortinet FortiOS Handbook: CLI Reference

#### NEW QUESTION 19

Which configuration can be used to reduce the number of BGP sessions in an 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 20

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

- A. You must disable add-route in the hub.
- B. All FortiGate 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 25**

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 29**

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-enforce-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 30**

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
10.1.40.0/24	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 31**

Which, three conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

- A. OSPF interface network types match
- B. OSPF router IDs are unique
- C. OSPF interface priority settings are unique
- D. OSPF link costs match
- E. Authentication settings match

**Answer:** ABE

**Explanation:**

? Option A is correct because the OSPF interface network types determine how the routers form adjacencies and exchange LSAs on a network segment. The network types must match for the routers to become neighbors1.

? Option B is correct because the OSPF router IDs are used to identify each router in the OSPF domain and to establish adjacencies. The router IDs must be unique for the routers to become neighbors2.

? Option E is correct because the authentication settings control how the routers authenticate each other before exchanging OSPF packets. The authentication settings must match for the routers to become neighbors3.

? Option C is incorrect because the OSPF interface priority settings are used to elect the designated router (DR) and the backup designated router (BDR) on a broadcast or non-broadcast multi-access network. The priority settings do not have to be unique for the routers to become neighbors, but they affect the DR/BDR election process4.

? Option D is incorrect because the OSPF link costs are used to calculate the shortest path to a destination network based on the bandwidth of the links. The link costs do not have to match for the routers to become neighbors, but they affect the routing decisions5. References: =

- ? 1: OSPF network types
- ? 2: OSPF router ID
- ? 3: OSPF authentication
- ? 4: OSPF interface priority
- ? 5: OSPF link cost

**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

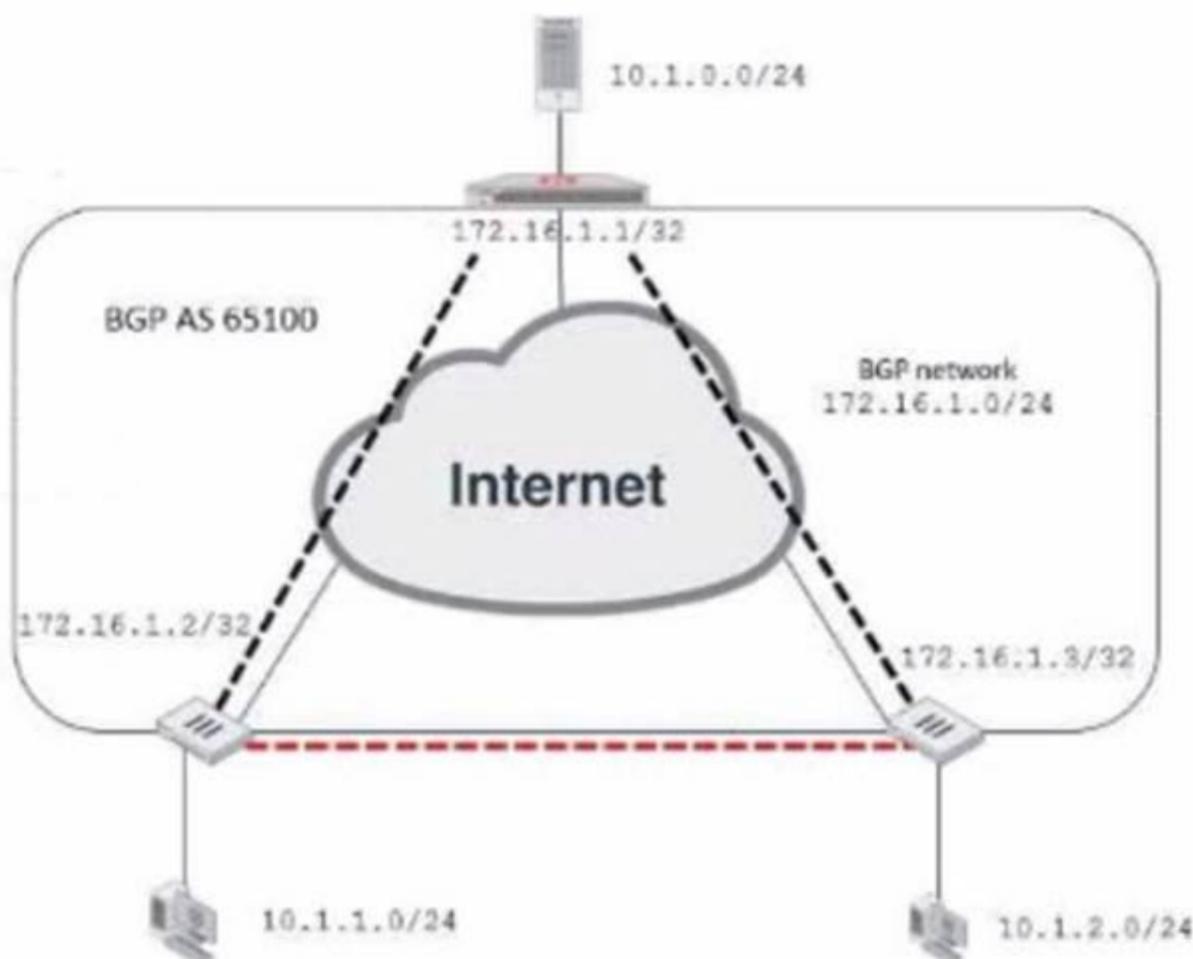
**Explanation:**

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 34**

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 39**

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

**Answer:** AC

**Explanation:**

For an ADVPN spoke configuration shown, the corresponding hub must have auto-discovery-sender enabled to send shortcut advertisement messages to the spokes. Also, the hub would need to have auto-discovery-forwarder enabled 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. The ike-version does not need to be reconfigured on the hub if it's already set to version 2 and auto-discovery-receiver is not necessary on the hub because it's the one sending the advertisements, not receiving.

References:

? FortiOS Handbook - ADVPN

**NEW QUESTION 40**

.....

## **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](#)**