



**Fortinet**

## **Exam Questions NSE7\_EFW-7.2**

Fortinet NSE 7 - Enterprise Firewall 7.2

### NEW QUESTION 1

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 2

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 root FortiGate sends
- D. Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer

**Answer:** BC

#### Explanation:

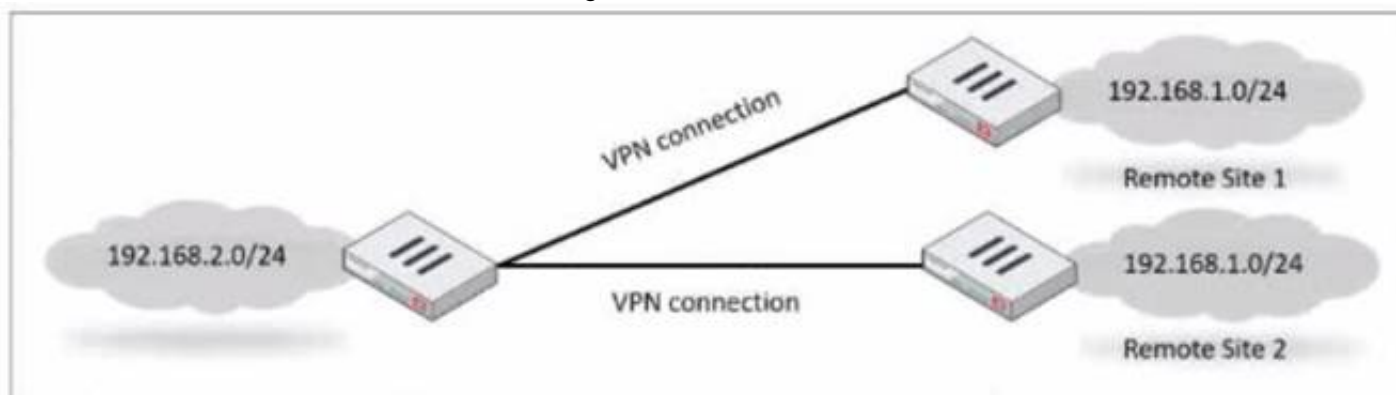
In the Security Fabric, only the root FortiGate sends logs to FortiAnalyzer (B). Additionally, only FortiGate devices with configuration-sync enabled receive and synchronize global Central Management Database (CMDB) objects that the root FortiGate sends (C). FortiGate uses the FortiTelemetry protocol 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 3

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 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=1454/00 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 cc8894be3390983521a48b2e7a5c998e6b28a10a3ddd8e7bc7ecbe672dfe7cc5
  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_rgwy=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:

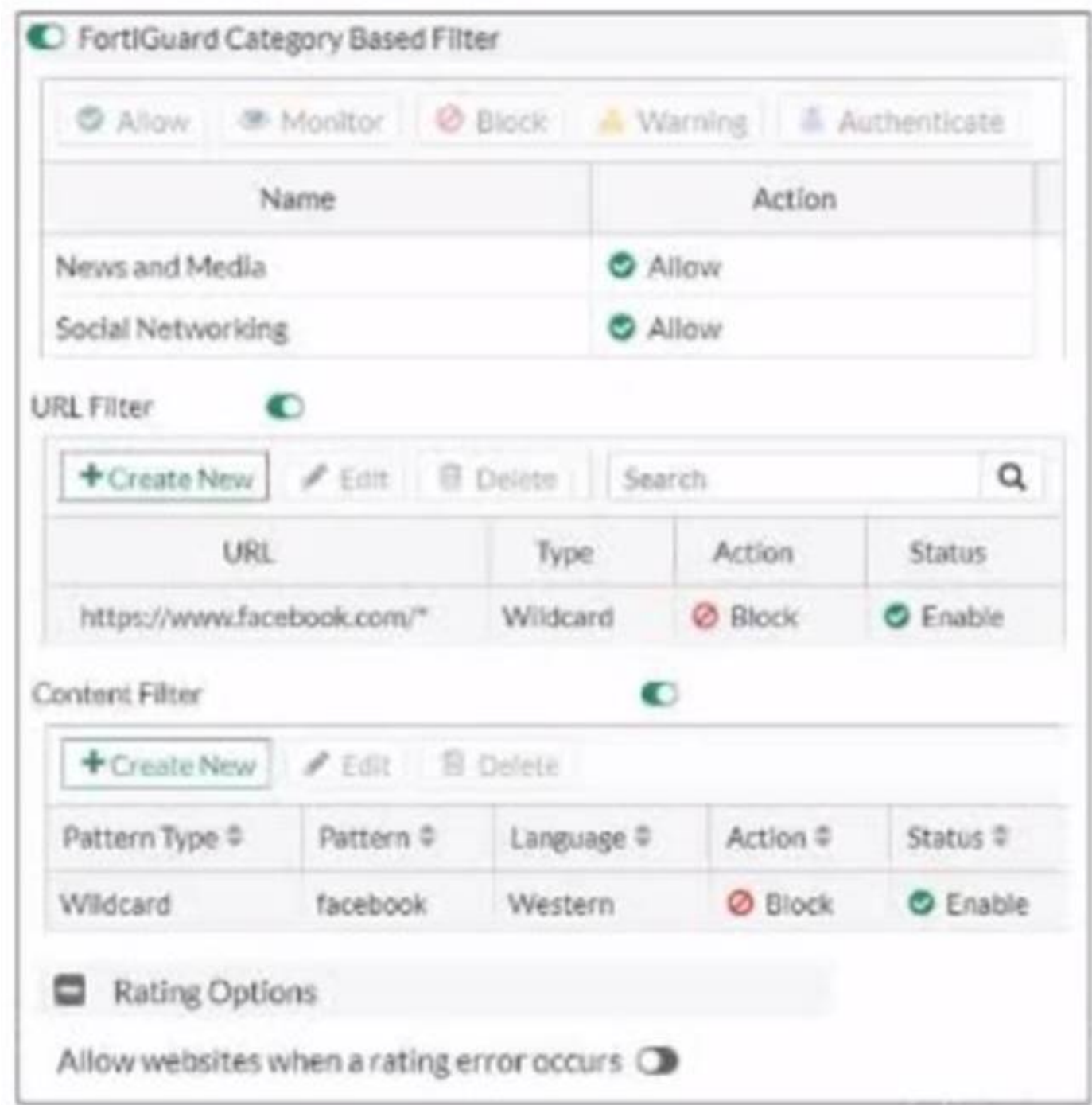
\* B. The IKE version is 2: This can be deduced from the presence of 'ver=2' in the output, which indicates that IKEv2 is being used.

\* 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**

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 6

Exhibit.



Refer to the exhibit, which shows information about an OSPF interface. What two conclusions can you draw from this command output? (Choose two.)

- A. The port3 network has more than one OSPF router



- B. The OSPF routers are in the area ID of 0.0.0.1.
- C. The interfaces of the OSPF routers match the MTU value that is configured as 1500.
- D. NGFW-1 is the designated router

**Answer:** AC

**Explanation:**

From the OSPF interface command output, we can conclude that the port3 network has more than one OSPF router because the Neighbor Count is 2, indicating the presence of another OSPF router besides NGFW-1. Additionally, we can deduce that the interfaces of the OSPF routers match the MTU value configured as 1500, which is necessary for OSPF neighbors to form adjacencies. The MTU mismatch would prevent OSPF from forming a neighbor relationship.

References:

? Fortinet FortiOS Handbook: OSPF Configuration

**NEW QUESTION 7**

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 8**

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

- 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:** AD

**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.

**NEW QUESTION 9**

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 10**

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 10**

Which FortiGate in a Security Fabric sends logs to FortiAnalyzer?

- A. Only the root FortiGate.
- B. Each FortiGate in the Security fabric.
- C. The FortiGate devices performing network address translation (NAT) or unified threat management (UTM). if configured.
- D. Only the last FortiGate that handled a session in the Security Fabric

**Answer:** B

**Explanation:**

? Option B is correct because each FortiGate in the Security Fabric can send logs to FortiAnalyzer for centralized logging and analysis<sup>12</sup>. This allows you to monitor and manage the entire Security Fabric from a single console and view aggregated reports and dashboards.

? Option A is incorrect because the root FortiGate is not the only device that can send logs to FortiAnalyzer. The root FortiGate is the device that initiates the Security Fabric and acts as the central point of contact for other FortiGate devices<sup>3</sup>. However, it does not have to be the only log source for FortiAnalyzer.

? Option C is incorrect because the FortiGate devices performing NAT or UTM are not the only devices that can send logs to FortiAnalyzer. These devices can perform additional security functions on the traffic that passes through them, such as firewall, antivirus, web filtering, etc<sup>4</sup>. However, they are not the only devices that generate logs in the Security Fabric.

? Option D is incorrect because the last FortiGate that handled a session in the Security Fabric is not the only device that can send logs to FortiAnalyzer. The last

FortiGate is the device that terminates the session and applies the final security policy<sup>5</sup>. However, it does not have to be the only device that reports the session information to FortiAnalyzer. References: =  
? 1: Security Fabric - Fortinet Documentation<sup>1</sup>  
? 2: FortiAnalyzer Demo<sup>6</sup>  
? 3: Security Fabric topology  
? 4: Security Fabric UTM features  
? 5: Security Fabric session handling

NEW QUESTION 14  
Exhibit.

Edit Policy

Name ⓘ

Internet\_Access

Policy Mode ⓘ

Standard

Learn Mode

Incoming Interface

port3

Outgoing Interface

port1

Source

all

+

Destination

all

+

Schedule

always

Service

App Default

Specify

Application

DNS

FTP

LinkedIn

+

URL Category

+

Action

✓ ACCEPT

⊘ DENY

Firewall/Network Options

Protocol Options

PROT default

Security Profiles

Refer to the exhibit, which contains a partial policy configuration. Which setting must you configure to allow SSH?

- A. Specify SSH in the Service field
- B. Configure port 22 in the Protocol Options field.
- C. Include SSH in the Application field
- D. Select an application control profile corresponding to SSH in the Security Profiles section

Answer: A

Explanation:

? Option A is correct because to allow SSH, you need to specify SSH in the Service field of the policy configuration. This is because the Service field determines which types of traffic are allowed by the policy<sup>1</sup>. By default, the Service field is set to App Default, which means that the policy will use the default ports defined by the applications. However, SSH is not one of the default applications, so you need to specify it manually or create a custom service for it<sup>2</sup>.  
? Option B is incorrect because configuring port 22 in the Protocol Options field is not enough to allow SSH. The Protocol Options field allows you to customize the protocol inspection and anomaly protection settings for the policy<sup>3</sup>. However, this field does not override the Service field, which still needs to match the traffic type.  
? Option C is incorrect because including SSH in the Application field is not enough to allow SSH. The Application field allows you to filter the traffic based on the application signatures and categories<sup>4</sup>. However, this field does not override the Service field, which still needs to match the traffic type.



? Option D is incorrect because selecting an application control profile corresponding to SSH in the Security Profiles section is not enough to allow SSH. The Security Profiles section allows you to apply various security features to the traffic, such as antivirus, web filtering, IPS, etc. However, this section does not override the Service field, which still needs to match the traffic type. References: =

? 1: Firewall policies

? 2: Services

? 3: Protocol options profiles

? 4: Application control

#### NEW QUESTION 15

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?

- 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:

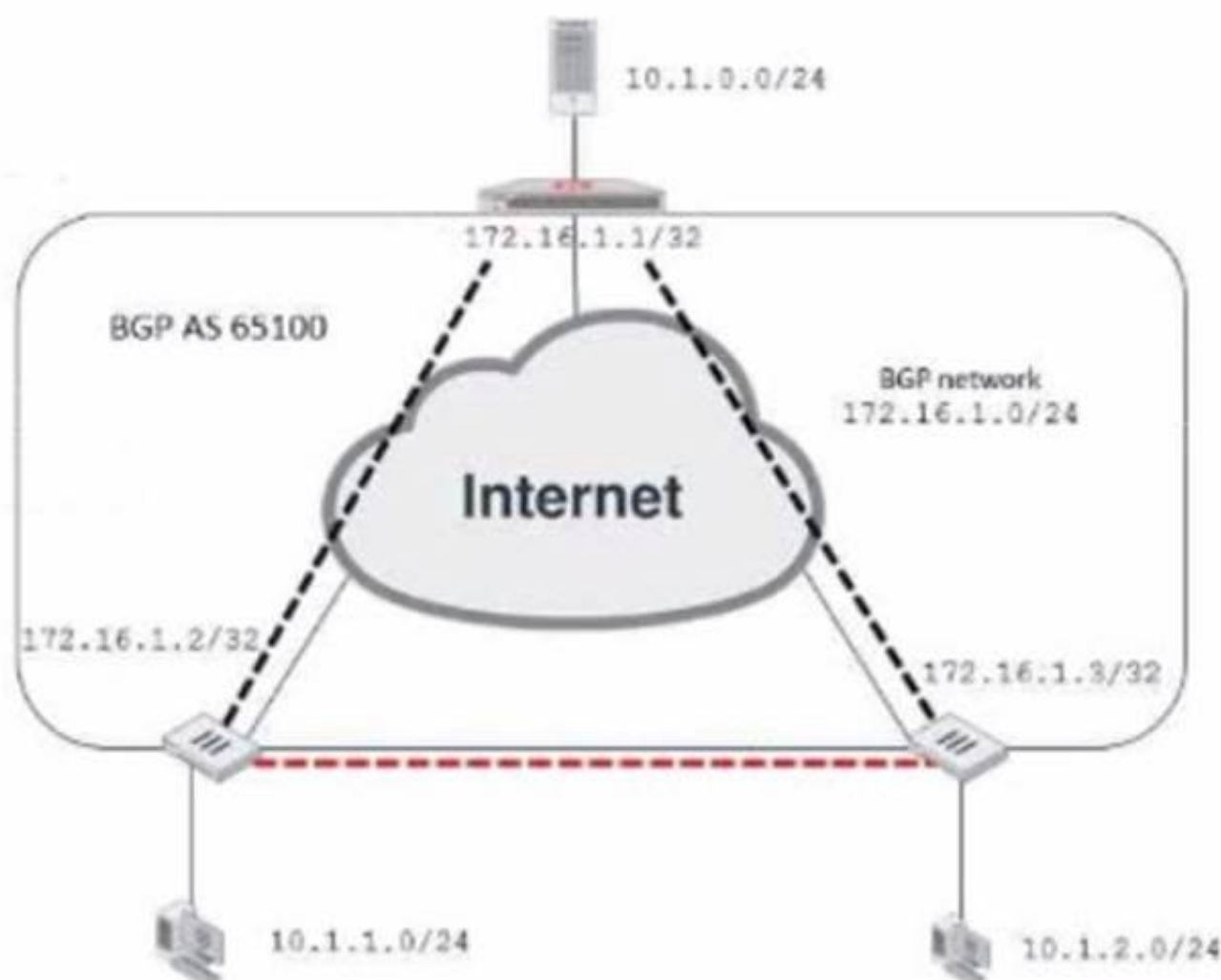
\* B. The router sends grace LSAs before it restarts: This is implied by the command 'set restart-mode graceful-restart'. When OSPF is configured with graceful restart, the router sends grace LSAs (Link State Advertisements) to inform its neighbors that it is restarting, allowing for a seamless transition 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.

#### NEW QUESTION 16

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 the 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 18

.....

## 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](#)**