



## **Fortinet**

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

Fortinet NSE 7 - Enterprise Firewall 7.2

## About ExamBible

### [Your Partner of IT Exam](#)

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

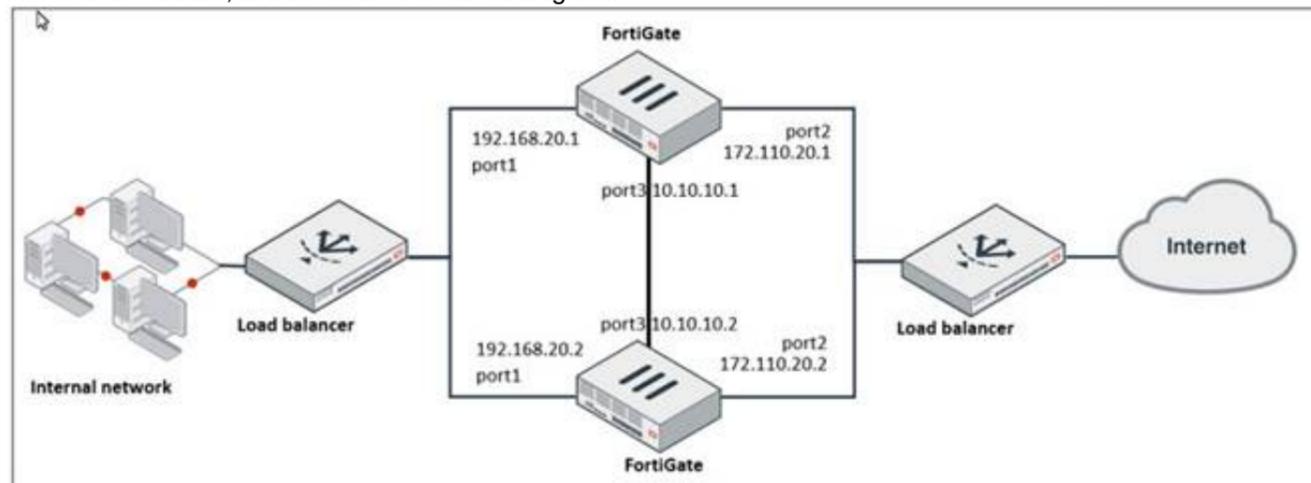
Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### 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

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 4

Which 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 5**

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:**

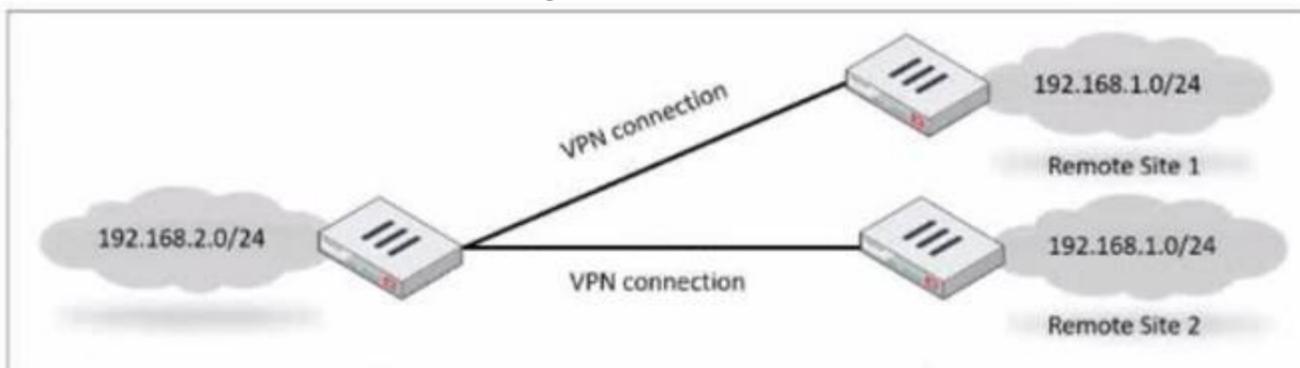
In the Security Fabric, only the root FortiGate sends logs to FortiAnalyzer (B). Additionally, only FortiGate devices with configuration-sync enabled receive and synchronize global Central Management Database (CMDB) objects that the root FortiGate sends (C). FortiGate uses the FortiTelemetry protocol 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 6**

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 7**

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_
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=877d6598 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 8**

Exhibit.

```
NGFW-1 # get router info ospf interface
port3 is up, line protocol is up
  Internet Address 10.1.0.254/24, Area 0.0.0.0, MTU 1500
  Process ID 0, VRF 0, Router ID 0.0.0.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROther, Priority 1
  Designated Router (ID) 0.0.0.3, Interface Address 10.1.0.1
  Backup Designated Router (ID) 0.0.0.2, Interface Address 10.1.0.100
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:08
  Neighbor Count is 2, Adjacent neighbor count is 2
  Crypt Sequence Number is 21
  Hello received 412 sent 207, DD received 8 sent 8
  LS-Req received 2 sent 3, LS-Upd received 13 sent 6
  LS-Ack received 9 sent 7, Discarded 6
```

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

- A. The port3 network has more man 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 9**

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 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 peers1. BFD can be enabled on both connected FortiGate devices by using the command set bfd enable under the BGP configuration2. References: =

Technical Tip :

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

### 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 13

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. IKE version 2 also exchanges a minimum of four messages to establish a secure tunnel, which is more efficient than IKE version 1.2. References: = IKE settings | FortiClient 7.2.2 - Fortinet

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

### NEW QUESTION 17

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 21

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 22**

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 23**

You created a VPN community using VPN Manager on FortiManager. You also added gateways to the VPN community. Now you are trying to create firewall policies to permit traffic over the tunnel however, the VPN interfaces do not appear as available options.

- A. Create interface mappings for the IPsec VPN interfaces before you use them in a policy.
- B. Refresh the device status using the Device Manager so that FortiGate populates the IPsec interfaces
- C. Configure the phase 1 settings in the VPN community that you didnt initially configur
- D. FortiGate automatically generates the interfaces after you configure the required settings
- E. install the VPN community and gateway configuration on the fortiGate devices so that the VPN interfaces appear on the Policy Objects on fortiManager.

**Answer: D**

**Explanation:**

To use the VPN interfaces in a policy, you need to install the VPN community and gateway configuration on the FortiGate devices first. This will create the VPN interfaces on the FortiGate and sync them with FortiManager. References:

- ? Creating IPsec VPN communities
- ? VPN | FortiGate / FortiOS 7.2.0

**NEW QUESTION 24**

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 26**

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	port2	0	Connected
172.16.100.0/24	0.0.0.0	port3	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**

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.

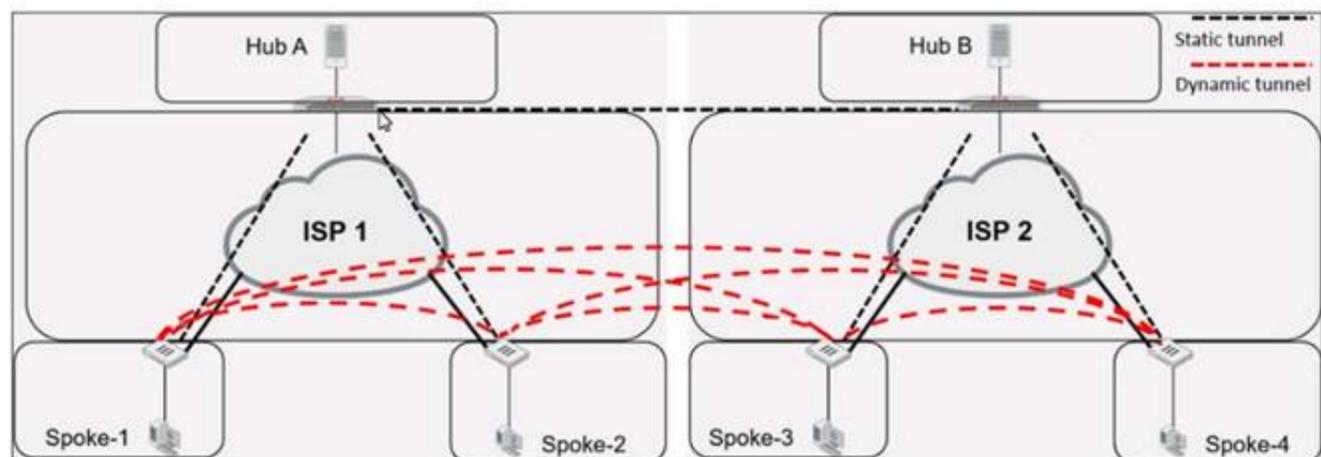
**Answer:** D

**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.fortiguar.net) needs to be configured.

**NEW QUESTION 33**

Refer to the exhibit, which shows an ADVPN network.



Which VPN phase 1 parameters must you configure on the hub for the ADVPN feature to function? (Choose two.)

- A. set auto-discovery-forwarder enable
- B. set add-route enable
- C. set auto-discovery-receiver enable
- D. set auto-discovery-sender enable

**Answer:** AC

**Explanation:**

For the ADVPN feature to function properly on the hub, the following phase 1 parameters must be configured:

- \* A. set auto-discovery-forwarder enable: This enables the hub to forward shortcut information to the spokes, which is essential for them to establish direct tunnels.
- \* C. set auto-discovery-receiver enable: This allows the hub to receive shortcut offers from the spokes.

This information is corroborated by the Fortinet documentation, which explains that in an ADVPN setup, the hub must be able to both forward and receive shortcut information for dynamic tunnel creation between spokes.

**NEW QUESTION 35**

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:

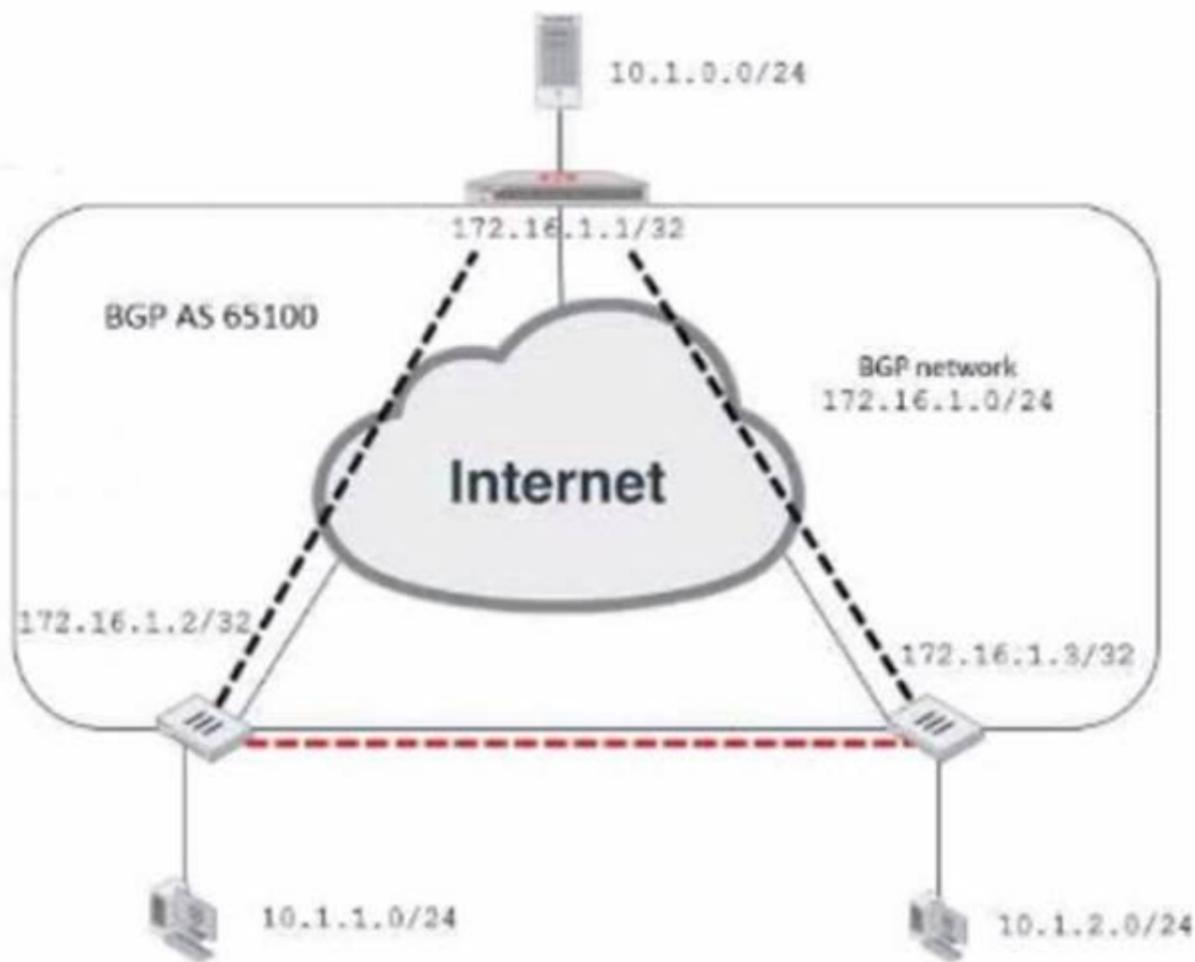
\* B. The router sends grace LSAs before it restarts: This is implied by the command 'set restart-mode graceful-restart'. When OSPF is configured with graceful restart, the router sends grace LSAs (Link State Advertisements) to inform its neighbors that it is restarting, allowing for a seamless transition 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 37**

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 41

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 43**

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 48**

.....

## Relate Links

**100% Pass Your NSE7\_EFW-7.2 Exam with ExamBible Prep Materials**

[https://www.exambible.com/NSE7\\_EFW-7.2-exam/](https://www.exambible.com/NSE7_EFW-7.2-exam/)

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>