

## Exam Questions NSE7\_EFW-7.2

Fortinet NSE 7 - Enterprise Firewall 7.2

[https://www.2passeasy.com/dumps/NSE7\\_EFW-7.2/](https://www.2passeasy.com/dumps/NSE7_EFW-7.2/)



## NEW QUESTION 1

Exhibit.

```
Routing table for VRF=0
B*  0.0.0.0/0 [20/0] via 100.64.1.254 (recursive is directly connected, port1), 00:03:58, [1/0]
C   10.1.0.0/24 is directly connected, port3
B   10.1.1.0/24 [200/0] via 172.16.1.2 (recursive is directly connected, tunnel_0), 00:03:25, [1/0]
B   10.1.2.0/24 [200/0] via 172.16.1.3 (recursive is directly connected, tunnel_1), 00:03:21, [1/0]
O   10.1.4.0/24 [110/2] via 10.1.0.100, port3, 00:04:56, [1/0]
O   10.1.10.0/24 [110/2] via 10.1.0.1, port3, 00:04:56, [1/0]
C   100.64.1.0/24 is directly connected, port1
C   100.64.2.0/24 is directly connected, port2
C   172.16.1.1/32 is directly connected, tunnel_0
      is directly connected, tunnel_1
C   172.16.1.2/32 is directly connected, tunnel_0
C   172.16.1.3/32 is directly connected, tunnel_1
C   172.16.100.0/24 is directly connected, port8
```

Refer to the exhibit, which shows a partial routing table

What two conclusions can you draw from the corresponding FortiGate configuration? (Choose two.)

- A. IPsec Tunnel aggregation is configured
- B. net-device is enabled in the tunnel IPsec phase 1 configuration
- C. OSPF is configured to run over IPsec.
- D. add-route is disabled in the tunnel IPsec phase 1 configuration.

**Answer: BD**

### Explanation:

? Option B is correct because the routing table shows that the tunnel interfaces have a netmask of 255.255.255.255, which indicates that net-device is enabled in the phase 1 configuration. This option allows the FortiGate to use the tunnel interface as a next-hop for routing, without adding a route to the phase 2 destination<sup>1</sup>.

? Option D is correct because the routing table does not show any routes to the phase 2 destination networks, which indicates that add-route is disabled in the phase 1 configuration. This option controls whether the FortiGate adds a static route to the phase 2 destination network using the tunnel interface as the gateway<sup>2</sup>.

? Option A is incorrect because IPsec tunnel aggregation is a feature that allows multiple phase 2 selectors to share a single phase 1 tunnel, reducing the number of tunnels and improving performance<sup>3</sup>. This feature is not related to the routing table or the phase 1 configuration.

? Option C is incorrect because OSPF is a dynamic routing protocol that can run over IPsec tunnels, but it requires additional configuration on the FortiGate and the peer device<sup>4</sup>. This option is not related to the routing table or the phase 1 configuration. References: =

? 1: Technical Tip: 'set net-device' new route-based IPsec logic<sup>2</sup>

? 2: Adding a static route<sup>5</sup>

? 3: IPsec VPN concepts<sup>6</sup>

? 4: Dynamic routing over IPsec VPN<sup>7</sup>

## NEW QUESTION 2

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 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 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 4

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 5**

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 6

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 7

Which two statements about IKE vision 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 1.2. References: = IKE settings | FortiClient 7.2.2 - Fortinet Documentation, Technical Tip: How to configure IKE version 1 or 2 ... - Fortinet Community

**NEW QUESTION 8**

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 9**

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 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

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7\_EFW-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7\_EFW-7.2 Product From:

[https://www.2passeasy.com/dumps/NSE7\\_EFW-7.2/](https://www.2passeasy.com/dumps/NSE7_EFW-7.2/)

## Money Back Guarantee

### **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