

NSE7_EFW-7.2^{Q&As}

Fortinet NSE 7 - Enterprise Firewall 7.2

Pass Fortinet NSE7_EFW-7.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/nse7_efw-7-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

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

Correct Answer: AD

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

QUESTION 2

In which two ways does FortiManager function when it is deployed as a local FDS? (Choose two)

- A. It can be configured as an update server a rating server or both
- B. It provides VM license validation services
- C. It supports rating requests from non-FortiGate devices.
- D. It caches available firmware updates for unmanaged devices

Correct Answer: AB


When deployed as a local FortiGuard Distribution Server (FDS), FortiManager functions in several capacities. It can act as an update server, a rating server, or both, providing firmware updates and FortiGuard database updates. Additionally, it plays a crucial role in VM license validation services, ensuring that the connected FortiGate devices are

operating with valid licenses. However, it does not support rating requests from non-FortiGate devices nor cache firmware updates for unmanaged devices. Fortinet FortiOS Handbook: FortiManager as a Local FDS Configuration


QUESTION 3

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

Engineering address object

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

Finance address object

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

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.

Correct Answer: B

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.

QUESTION 4

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

A. It allows failure detection in less than one second.

B. The two routers must be connected to the same subnet.

C. It is supported for neighbors over multiple hops.

D. It detects only two-way failures.

Correct Answer: AC

Bidirectional Forwarding Detection (BFD) is a rapid protocol for detecting failures in the forwarding path between two adjacent routers, including interfaces, data links, and forwarding planes. BFD is designed to detect forwarding path failures in a very short amount of time, often less than one second, which is significantly faster than traditional failure detection mechanisms like hold-down timers in routing protocols. Fortinet supports BFD for BGP, and it can be used over multiple hops, which allows the detection of failures even if the BGP peers are not directly connected. This functionality enhances the ability to maintain stable BGP sessions over a wider network topology and is documented in Fortinet's guides.

QUESTION 5

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.)

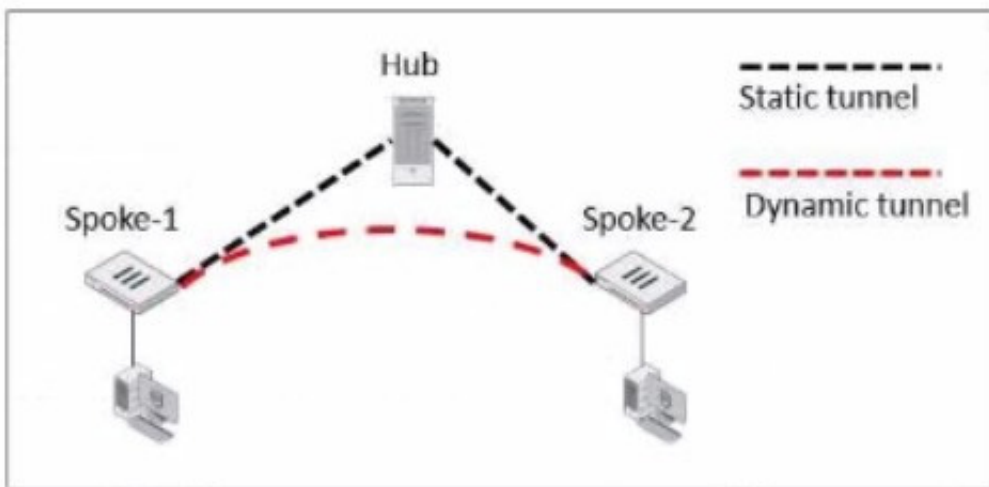
- A. Set auto-discovery-sender enable
- B. Set ike-version 2
- C. Set auto-discovery-forwarder enable
- D. Set auto-discovery-receiver enable

Correct Answer: AC

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

QUESTION 6

Exhibit.



Refer to the exhibit, which shows an ADVPN network.

The client behind Spoke-1 generates traffic to the device located behind Spoke-2.

Which first message does the hub send to Spoke-1 to bring up the dynamic tunnel?

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

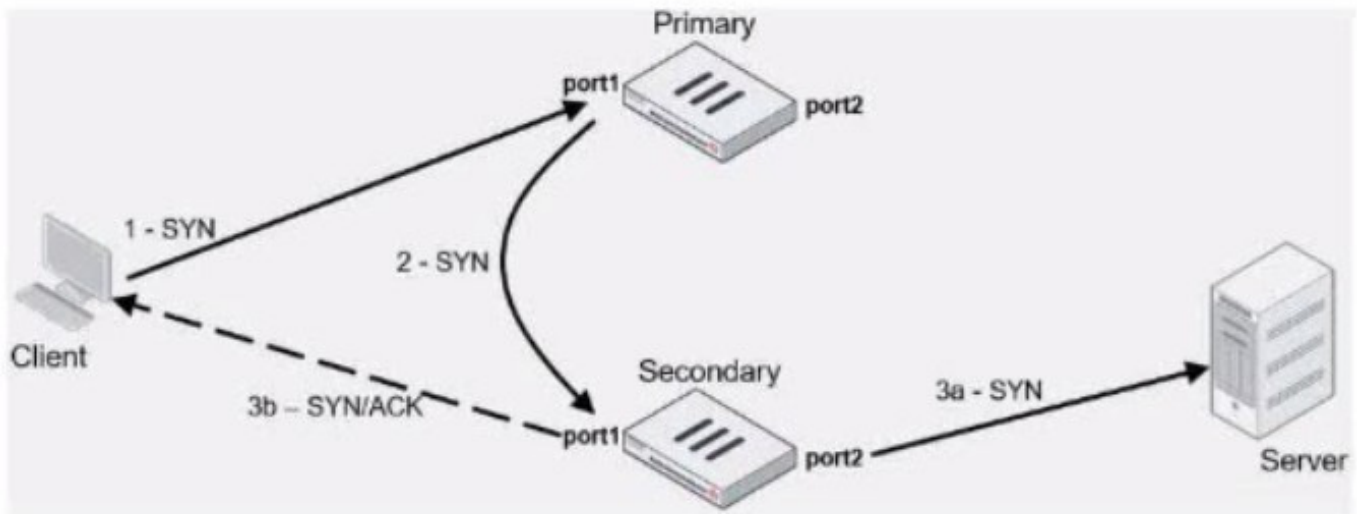
D. Shortcut forward

Correct Answer: A

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

QUESTION 7

Exhibit.



Refer to the exhibit, which contains an active-active load balancing scenario.

During the traffic flow the primary FortiGate forwards the SYN packet to the secondary FortiGate.

What is the destination MAC address or addresses when packets are forwarded from the primary FortiGate to the secondary FortiGate?

- A. Secondary physical MAC port1
- B. Secondary virtual MAC port1
- C. Secondary virtual MAC port1 then physical MAC port1
- D. Secondary physical MAC port2 then virtual MAC port2

Correct Answer: A

In an active-active load balancing scenario, when the primary FortiGate forwards the SYN packet to the secondary FortiGate, the destination MAC address would be the secondary's physical MAC on port1, as the packet is being sent over the network and the physical MAC is used for layer 2 transmissions.

QUESTION 8

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

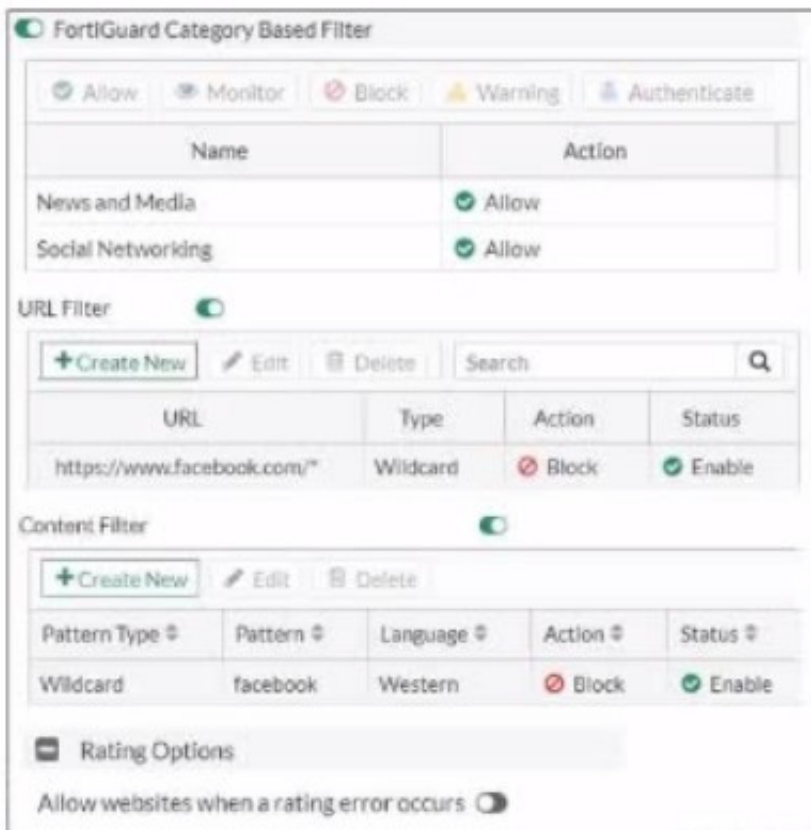
- A. You can configure it on the GUI.
- B. It applies common settings in an OSPF area.
- C. It is combined with the neighbor-range parameter.
- D. You can apply it in Internal BGP (IBGP) and External BGP (EBGP).

Correct Answer: BD

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.

QUESTION 9

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 hocked if the local or the public FortiGuard server does not reply

Correct Answer: C

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 section1. 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

QUESTION 10

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.

Correct Answer: AB

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

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.

[Latest NSE7_EFW-7.2 Dumps](#)

[NSE7_EFW-7.2 Exam Questions](#)

[NSE7_EFW-7.2 Braindumps](#)