

# Fortinet

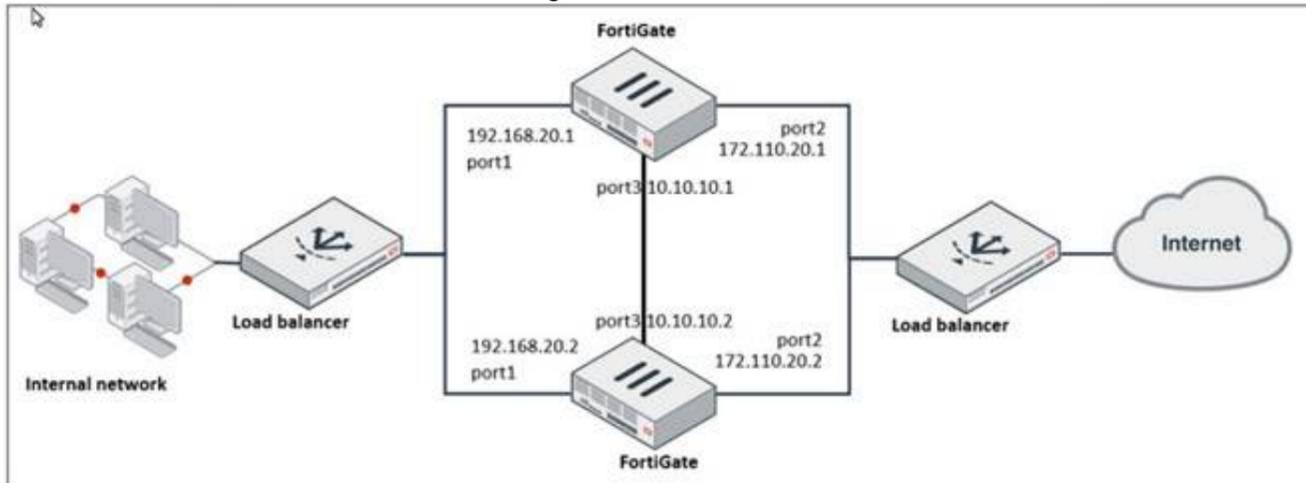
## Exam Questions NSE7\_EFW-7.2

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**

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**

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 4**

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 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**

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

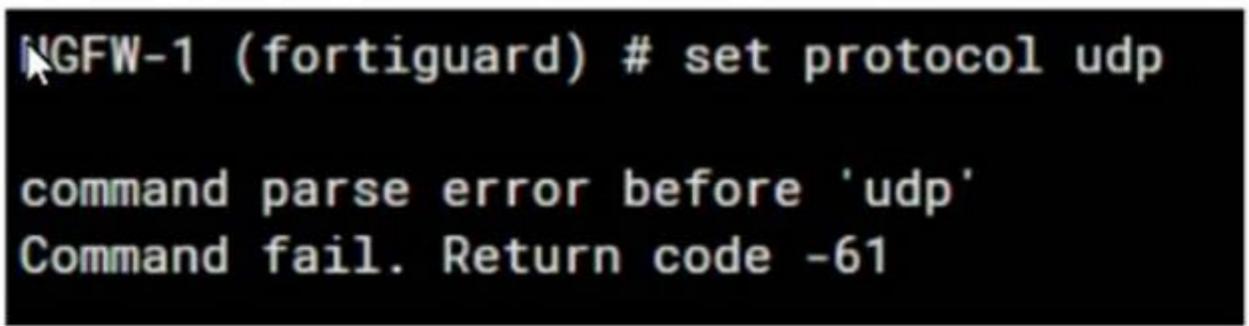
**Answer:** D

**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 7**

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



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 8**

Exhibit.

```

FortiGate-A (port4) # show
config system interface
  edit "port4"
    set vdom "root"
    set ip 10.1.5.1 255.255.255.0
    set allowaccess ping https
    set type physical
    set vrrp-virtual-mac enable
    config vrrp
      edit 1
        set vrgrp 1
        set vrip 10.1.5.254
        set priority 255
        set preempt enable
        set vrdst 8.8.8.8
        set vrdst-priority 30
      next
    end
  set snmp-index 4
next
end

FortiGate-B (port4) # show
config system interface
  edit "port4"
    set vdom "root"
    set ip 10.1.5.2 255.255.255.0
    set allowaccess ping https
    set type physical
    set vrrp-virtual-mac enable
    config vrrp
      edit 1
        set vrgrp 1
        set vrip 10.1.5.254
        set priority 50
        set preempt enable
        set vrdst 8.8.8.8
        set vrdst-priority 40
      next
    end
  set snmp-index 4
next
end

```

Refer to the exhibit, which contains the partial interface configuration of two FortiGate devices.

Which two conclusions can you draw from this configuration? (Choose two)

- A. 10.1.5.254 is the default gateway of the internal network
- B. On failover new primary device uses the same MAC address as the old primary
- C. The VRRP domain uses the physical MAC address of the primary FortiGate
- D. By default FortiGate B is the primary virtual router

**Answer: AB**

**Explanation:**

The Virtual Router Redundancy Protocol (VRRP) configuration in the exhibit indicates that 10.1.5.254 is set as the virtual IP (VRIP), commonly serving as the default gateway for the internal network (A). With vrrp-virtual-mac enabled, both FortiGates would use the same virtual MAC address, ensuring a seamless transition during failover (B). The VRRP domain does not use the physical MAC address (C), and the priority settings indicate that FortiGate-A would be the primary router by default due to its higher priority (D).

**NEW QUESTION 9**

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 10

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

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 11

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 16

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 17

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 20**

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 24**

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 29**

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**

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 39**

You want to improve reliability over a lossy IPSec tunnel.

Which combination of IPSec phase 1 parameters should you configure?

- A. fec-ingress and fec-egress
- B. Odpd and dpd-retryinterval
- C. fragmentation and fragmentation-mtu
- D. keepalive and keylive

**Answer: C**

**Explanation:**

For improving reliability over a lossy IPSec tunnel, the fragmentation and fragmentation-mtu parameters should be configured. In scenarios where there might be issues with packet size or an unreliable network, setting the IPsec phase 1 to allow for fragmentation will enable large packets to be broken down, preventing them from being dropped due to size or poor network quality. The fragmentation-mtu specifies the size of the fragments. This is aligned with Fortinet's recommendations for handling IPsec VPN over networks with potential packet loss or size limitations.

**NEW QUESTION 44**

.....

## **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](#)**