

# Fortinet

## Exam Questions NSE7\_EFW-7.2

Fortinet NSE 7 - Enterprise Firewall 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**

Refer to the exhibit, which shows a custom signature.

```

Signature
SBID( -name "Ultraviewer.Custom"; -protocol tcp; -service ssl; -flow from_client;
-pattern "ultraviewer"; -context host; -app_cat 7;)
    
```

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 3**

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**

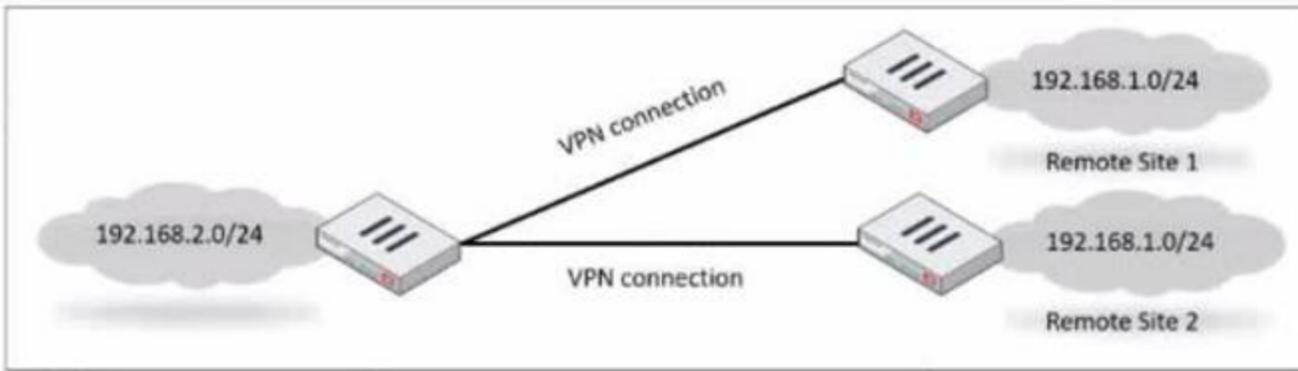
**Explanation:**

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 4**

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:**

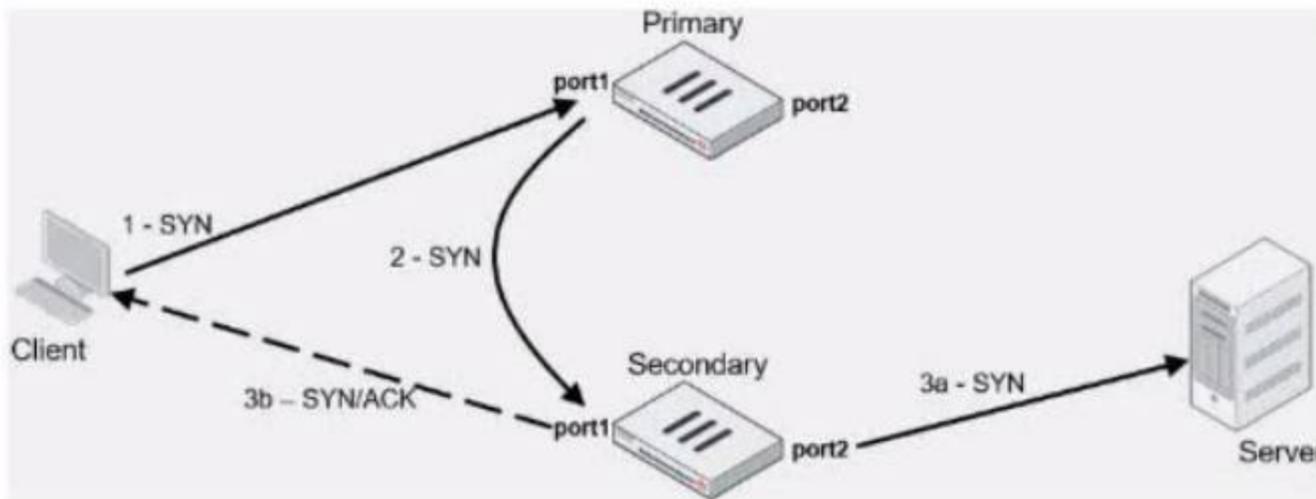
To ensure that only one remote site is connected at any given time in an IPsec VPN scenario, you should use route-overlap with the option to either use-new or use-old. This setting dictates which routes are preferred and how overlaps in routes are handled, allowing for one connection to take precedence over the other (C).

References:

? FortiOS Handbook - IPsec VPN

**NEW QUESTION 5**

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

**Answer: A**

**Explanation:**

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.

**NEW QUESTION 6**

Exhibit.

```
config vpn ipsec phase1-interface
edit tunnel
set type dynamic
set interface "port1"
set ike-version 2
set keylife 28800
set peertype any
set net-device disable
set proposal aes128-sha256 aes256-sha256
set dpd on-idle
set add-route enable
set psksecret fortinet
next
end
```

Refer to the exhibit, which contains a partial VPN configuration. What can you conclude from this configuration1?

- A. FortiGate creates separate virtual interfaces for each dial up client.
- B. The VPN should use the dynamic routing protocol to exchange routing information Through the tunnels.
- C. Dead peer detection s disabled.
- D. The routing table shows a single IPSec virtual interface.

**Answer: C**

**Explanation:**

The configuration line "set dpd on-idle" indicates that dead peer detection (DPD) is set to trigger only when the tunnel is idle, not actively disabled<sup>1</sup>. References: FortiGate IPSec VPN User Guide - Fortinet Document Library  
 From the given VPN configuration, dead peer detection (DPD) is set to 'on-idle', indicating that DPD is enabled and will be used to detect if the other end of the VPN tunnel is still alive when no traffic is detected. Hence, option C is incorrect. The configuration shows the tunnel set to type 'dynamic', which does not create separate virtual interfaces for each dial- up client (A), and it is not specified that dynamic routing will be used (B). Since this is a phase 1 configuration snippet, the routing table aspect (D) cannot be concluded from this alone.

**NEW QUESTION 7**

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.

**Answer: AC**

**Explanation:**

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.

**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**

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**

Which statement about network processor (NP) offloading is true?

- A. For TCP traffic FortiGate CPU offloads the first packets of SYN/ACK and ACK of the three-way handshake to NP
- B. The NP provides IPS signature matching
- C. You can disable the NP for each firewall policy using the command np-acceleration st to loose.
- D. The NP checks the session key or IPSec SA

**Answer: B**

**Explanation:**

Network processors (NPs) are specialized hardware within FortiGate devices that accelerate certain security functions. One of the primary functions of NPs is to provide IPS signature matching (B), allowing for high-speed inspection of traffic against a database of known threat signatures.

**NEW QUESTION 14**

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 didn't initially configure
- 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 19**

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 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 25**

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 29**

Exhibit.



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

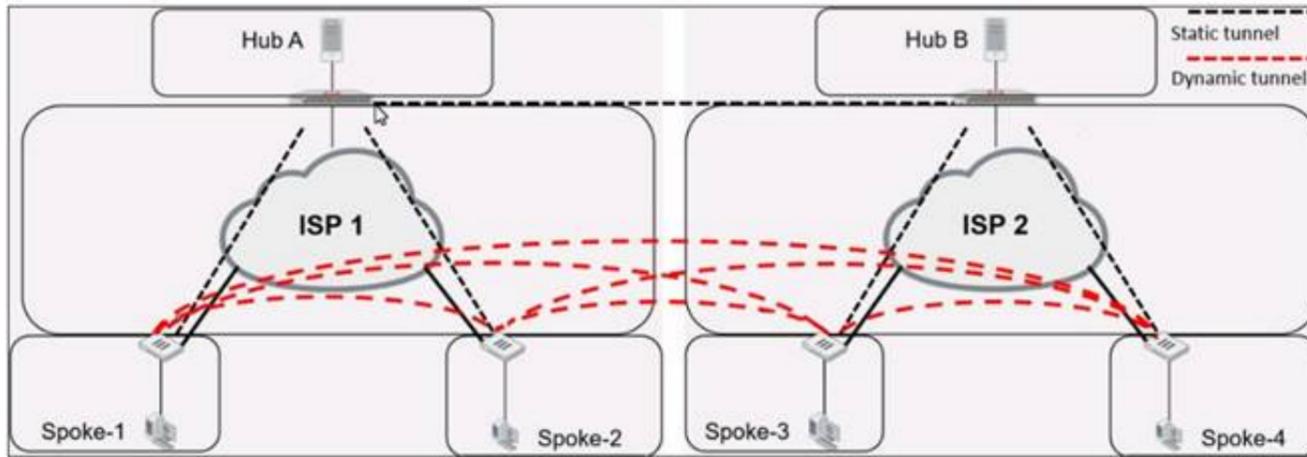
? 2: Services

? 3: Protocol options profiles

? 4: Application control

**NEW QUESTION 34**

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 38**

Exhibit.

Script Name	Static Route
Comments	<div style="border: 1px solid gray; height: 40px; width: 100%;"></div> 0/255
Type	CLI Script
Run script on	Remote FortiGate Directly (...)
Script details	<pre># conf rout stat #   edit 0 #     set gateway 10.20.121.2 #     set priority 20 #     set device "wan1" #   next # end</pre>

Refer to the exhibit, which contains a CLI script configuration on FortiManager. An administrator configured the CLI script on FortiManager but the script failed to apply any changes to the managed device after being executed.

What are two reasons why the script did not make any changes to the managed device? (Choose two)

- A. The commands that start with the # sign did not run.
- B. Incomplete commands can cause CLI scripts to fail.
- C. Static routes can be added using only TCI scripts.
- D. CLI scripts must start with #!.

**Answer:** AB

**Explanation:**

The commands that start with the # sign did not run because they are treated as comments in the CLI script. Incomplete commands can cause CLI scripts to fail because they are not recognized by the FortiGate device. The other options are incorrect because static routes can be added using CLI or GUI, and CLI scripts do not need to start with #!. References := Configuring custom scripts | FortiManager 7.2.0 - Fortinet Documentation, section "CLI script syntax".

**NEW QUESTION 43**

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:

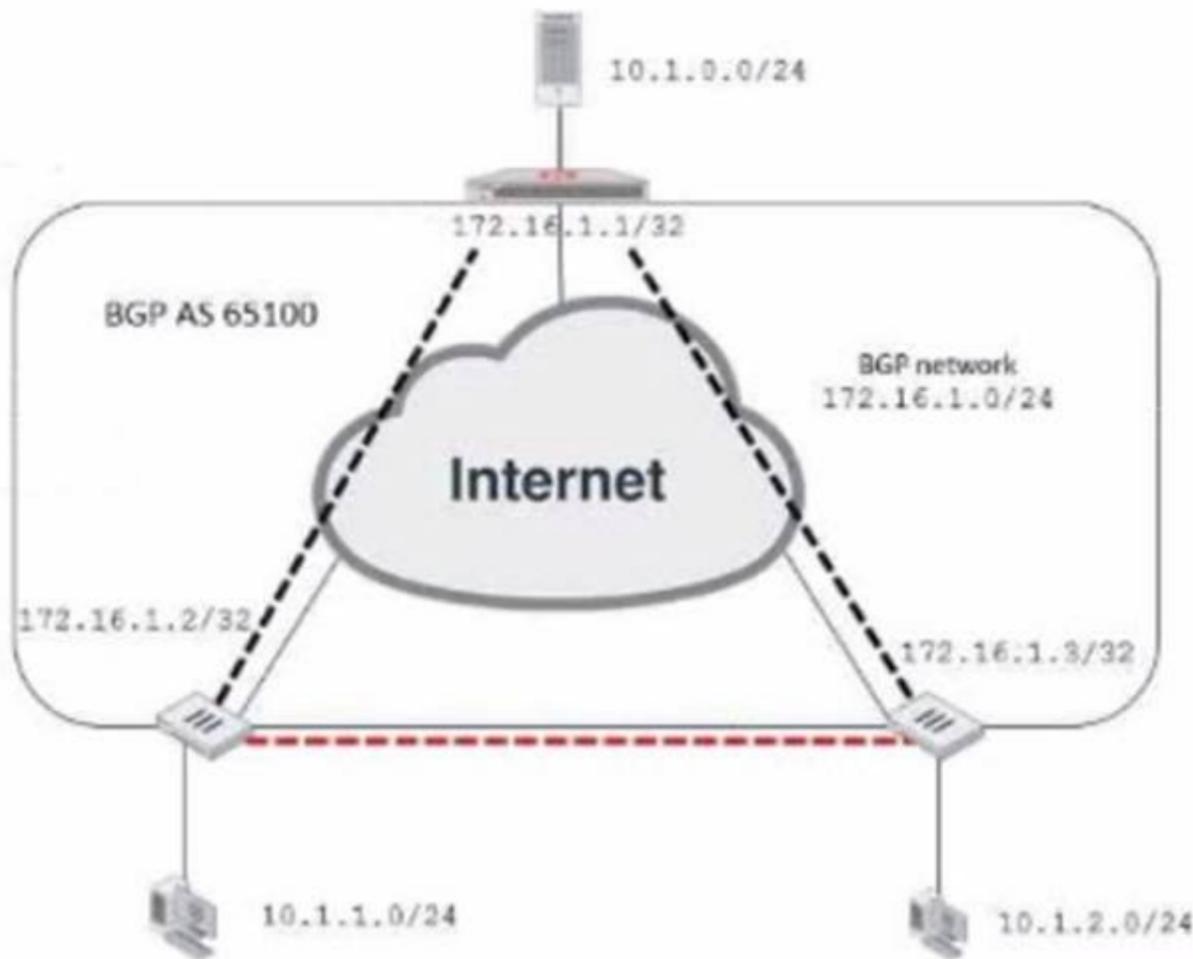
\* B. The router sends grace LSAs before it restarts: This is implied by the command 'set restart-mode graceful-restart'. When OSPF is configured with graceful restart, the router sends grace LSAs (Link State Advertisements) to inform its neighbors that it is restarting, allowing for a seamless transition 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 48**

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 53**

An administrator has configured two FortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device. What can the administrator do to fix this problem?

- A. Verify that the speed and duplex settings match between the FortiGate interfaces and the connected switch ports
- B. Configure set link-failed-signal enable under config system ha on both cluster members
- C. Configure remote link monitoring to detect an issue in the forwarding path
- D. Configure set send-garp-on-failover enables under config system ha on both cluster members

**Answer:** B

**Explanation:**

Virtual MAC Address and Failover

- The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port.
- Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces):

```
#Config system ha
```

```
set link-failed-signal enable end
```

- This simulates a link failure that clears the related entries from MAC table of the switches.

**NEW QUESTION 55**

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 59**

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 output1.

? 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 conversion2.

? 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 respectively3.

? 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 conversion2. References: =

? 1: Technical Tip: Verify the webfilter cache content4

? 2: Hexadecimal to Decimal Converter5

? 3: FortiGate - Fortinet Community6

? : Web filter | FortiGate / FortiOS 7.2.0 - Fortinet Documentation7

**NEW QUESTION 62**

.....

## **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](#)**