

# Fortinet

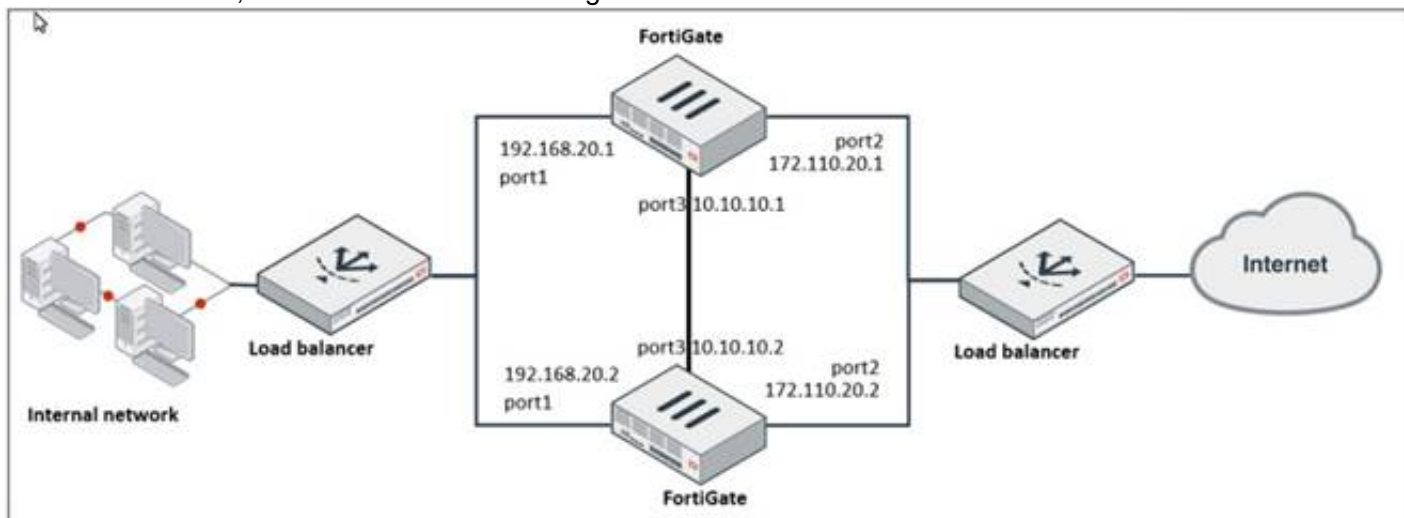
## Exam Questions NSE7\_EFW-7.2

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

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 destination1.  
 ? 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 gateway2.  
 ? 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 performance3. 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 device4. 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 logic2  
? 2: Adding a static route5  
? 3: IPSec VPN concepts6  
? 4: Dynamic routing over IPsec VPN7

**NEW QUESTION 4**

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 5**

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 disabled1. 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 6**

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

```
NGFW-1 (fortiguard) # set protocol udp
command parse error before 'udp'
Command fail. Return code -61
```

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 theconfig system fortiguardis 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 7

Exhibit.

FortiGate-A (port4) # show	FortiGate-B (port4) # show
config system interface	config system interface
edit "port4"	edit "port4"
set vdom "root"	set vdom "root"
set ip 10.1.5.1 255.255.255.0	set ip 10.1.5.2 255.255.255.0
set allowaccess ping https	set allowaccess ping https
set type physical	set type physical
set vrrp-virtual-mac enable	set vrrp-virtual-mac enable
config vrrp	config vrrp
edit 1	edit 1
set vrgrp 1	set vrgrp 1
set vrip 10.1.5.254	set vrip 10.1.5.254
set priority 255	set priority 50
set preempt enable	set preempt enable
set vrdest 8.8.8.8	set vrdest 8.8.8.8
set vrdest-priority 30	set vrdest-priority 40
next	next
end	end
set snmp-index 4	set snmp-index 4
next	next
end	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). Withvrrp-virtual-macenable, 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 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

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 interlaces
- D. Set protected network to all

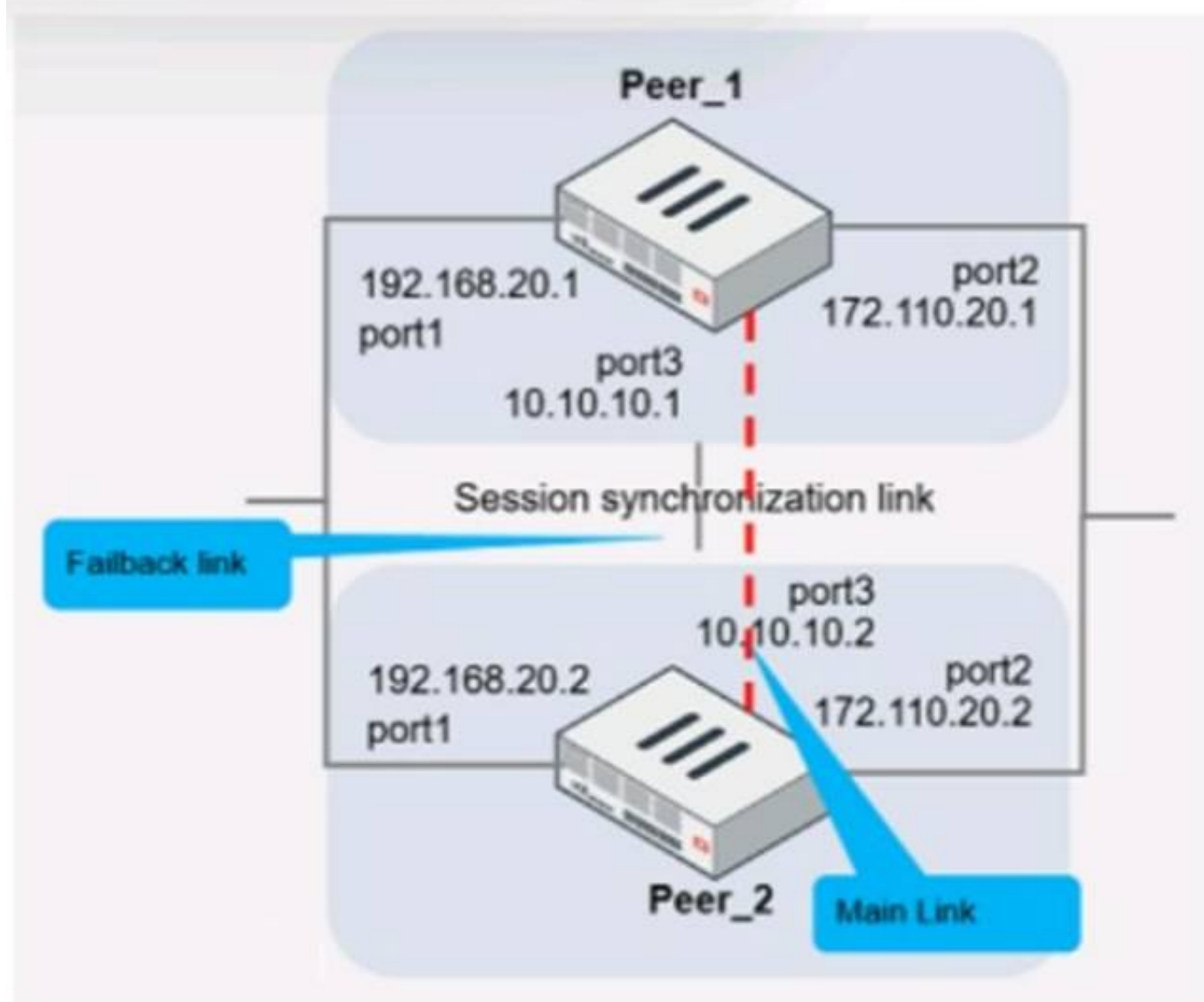
**Answer: A**

#### 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 10

Refer to the exhibit, which shows two configured FortiGate devices and peering over FGSP.



The main link directly connects the two FortiGate devices and is configured using the set session-syn-dev <interface> command.

What is the primary reason to configure the main link?

- A. To have both sessions and configuration synchronization in layer 2
- B. To load balance both sessions and configuration synchronization between layer 2 and 3
- C. To have only configuration synchronization in layer 3
- D. To have both sessions and configuration synchronization in layer 3

**Answer: D**

**Explanation:**

The primary purpose of configuring a main link between the devices is to synchronize session information so that if one unit fails, the other can continue processing traffic without dropping active sessions.

\* A.To have both sessions and configuration synchronization in layer 2.This is incorrect because FGSP is used for session synchronization, not configuration synchronization. B.To load balance both sessions and configuration synchronization between layer 2 and 3.FGSP does not perform load balancing and is not used for configuration synchronization.

\* C.To have only configuration synchronization in layer 3.The main link is not used solely for configuration synchronization.

\* D.To have both sessions and configuration synchronization in layer 3.The main link in an FGSP setup is indeed used to synchronize session information across the devices, and it operates at layer 3 since it uses IP addresses to establish the peering.

**NEW QUESTION 11**

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 12**

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 15**

Refer to the exhibit, which shows a routing table.

Network S	Gateway IP S	Interfaces S	Distance S	Type S
0.0.0.0	10.1.0.254	port1	10	Static
10.1.0.0/24	0.0.0.0	port1	0	Connected
10.1.4.0/24	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	port2	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 17**

Exhibit.

Script Name	Static Route
Comments	<div>0/255</div> <div>0/255</div>
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 rut the script tailed 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 19**

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 21**

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 26**

.....



## 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](#)**