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 touting table
What two concisions 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. OSPI 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 2
Refer to the exhibit, which contains information about an IPsec VPN tunnel.

```
FortiGate # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=tunnel_0 ver=2 serial=1 100.64.3.1:0->100.64.1.1:0 tun_id=100.64.1.1 tun_id6=::100.64.1.1
bound_if=3 lgwy=static/1 tun=intf mode=auto/1 encap=none/552 options[0228]=npu frag-rfc  run_s

proxyid_num=1 child_num=0 refcnt=3 ilast=42949917 olast=42949917 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=off on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec: egress=0 ingress=0
proxyid=tunnel_0_0 proto=0 sa=1 ref=2 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=30202 type=00 soft=0 mtu=1280 expire=1454/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 qat=192 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=1768/1800
  dec: spi=877d6590 esp=aes key=16 be308ec1fb05464205764424bc40a76d
       ah=sha256 key=32 cc8894be3390983521a48b2e7a5c998e6b28a10a3ddd8e7bc7ecbe672dfe7cc5
  enc: spi=63d0f38a esp=aes key=16 d8d3343af2fed4ddd958a022cd656b06
       ah=sha256 key=32 264402ba8ad04a7e97732b52ec27c92ff86e0a97bb33e22887677336f1670c7d
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
  npu_flag=00 npu_rgwy=100.64.1.1 npu_lgwy=100.64.3.1 npu_selid=0 dec_npuid=0 enc_npuid=0
run_tally=0
```

What two conclusions can you draw from the command output? (Choose two.)

A. Dead peer detection is set to enable.
B. The IKE version is 2.
C. Both IPsec SAs are loaded on the kernel.
D. Forward error correction in phase 2 is set to enable.

Answer: BC

Explanation:
From the command output shown in the exhibit:
* B. The IKE version is 2: This can be deduced from the presence of 'ver=2' in the output, which indicates that IKEv2 is being used.
* C. Both IPsec SAs are loaded on the kernel: This is indicated by the line 'npu flags=0x0/0', suggesting that no offload to NPU is occurring, and hence, both Security Associations are
loaded onto the kernel for processing.
Fortinet documentation specifies that the version of IKE (Internet Key Exchange) used and the loading of IPsec Security Associations can be verified through the

diagnostic commands related to VPN tunnels.

NEW QUESTION 3
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)

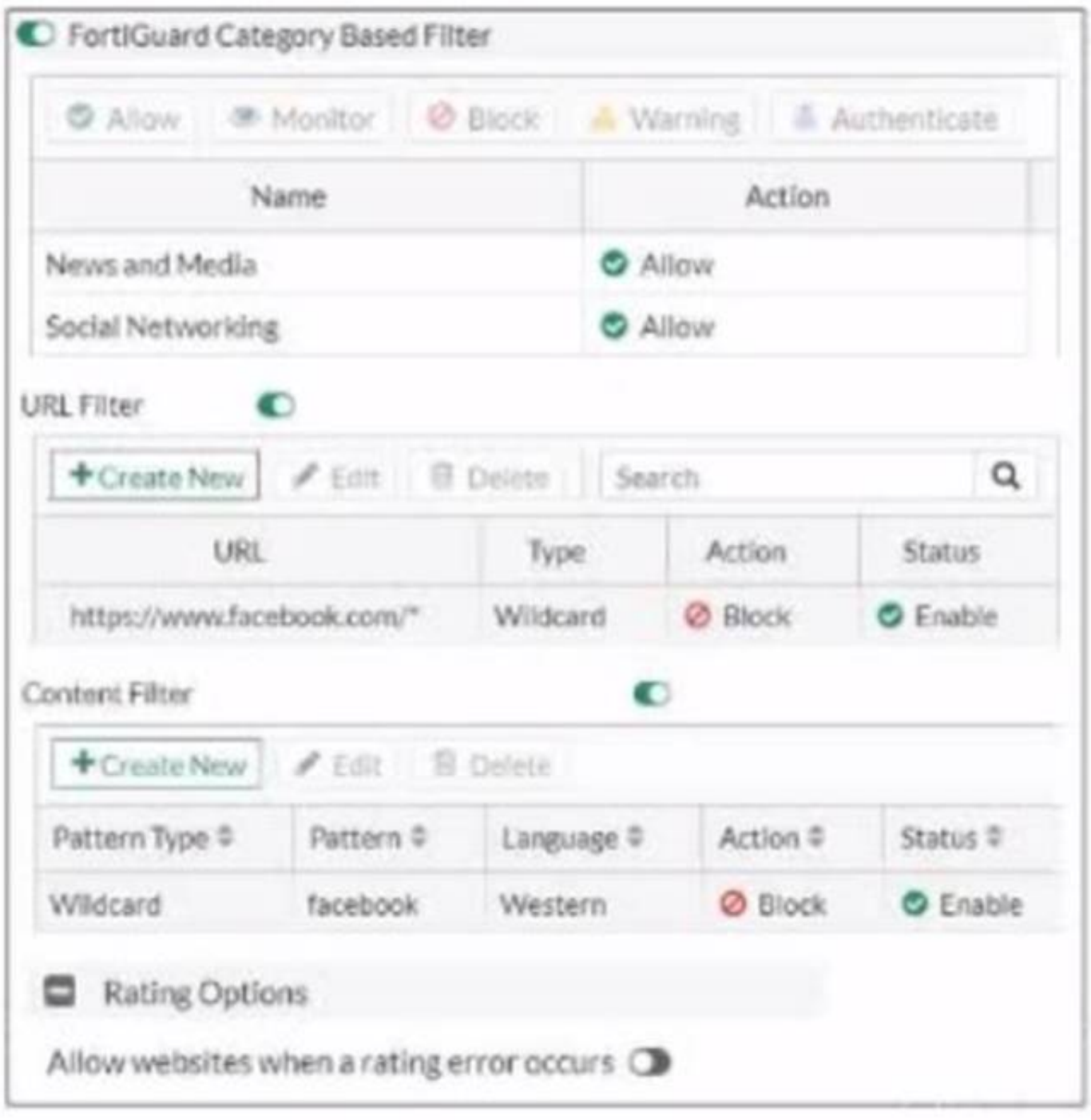
```
F-SBID( --name "eicar"; --protocol tcp; --service HTTP; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)
```

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 4
Exhibit.



Refer to the exhibit, which shows a partial web filter profile conjuration
What can you cone udo from this configuration about access towww.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

Answer: C

Explanation:
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

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
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
```

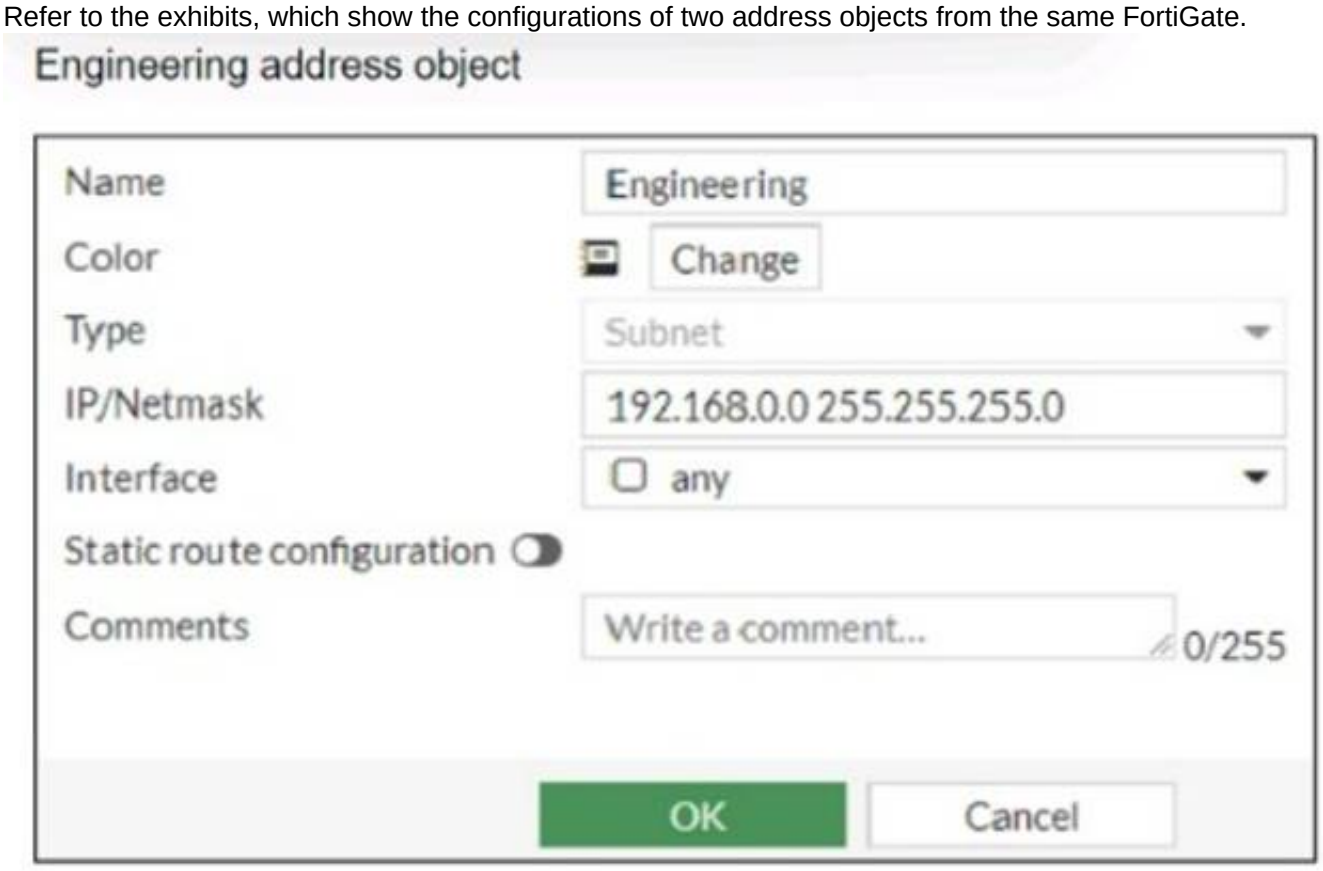
Refer to the exhibit, which contains the partial interface configuration of two FortiGate devices.
Which two conclusions can you draw from this con figuration? (Choose two)

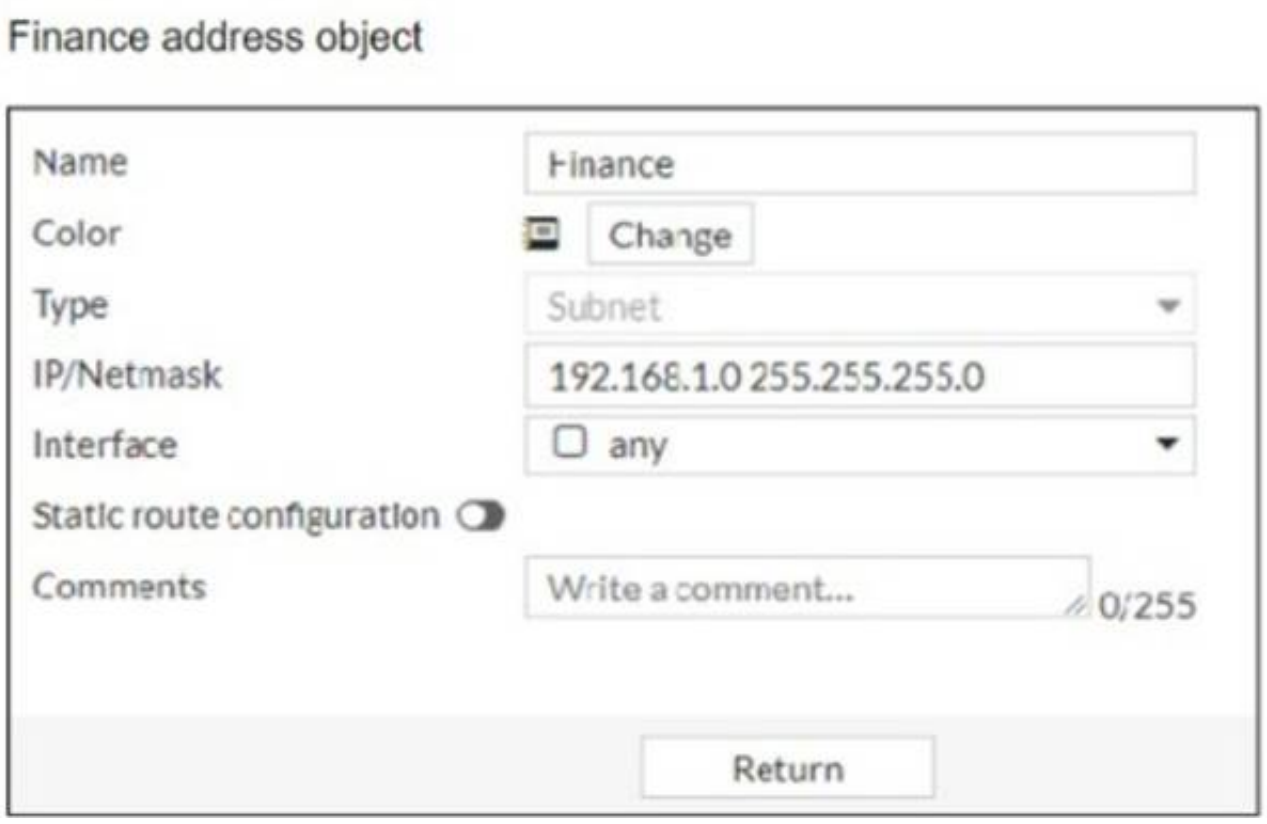
A. 10.1.5.254 is the default gateway of the internal network
B. On failover new primary device uses the same MAC address as the old primary
C. The VRRP domain uses the physical MAC address of the primary FortiGate
D. By default FortiGate B is the primary virtual router

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-macenabled, 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 7
Refer to the exhibits, which show the configurations of two address objects from the same FortiGate.





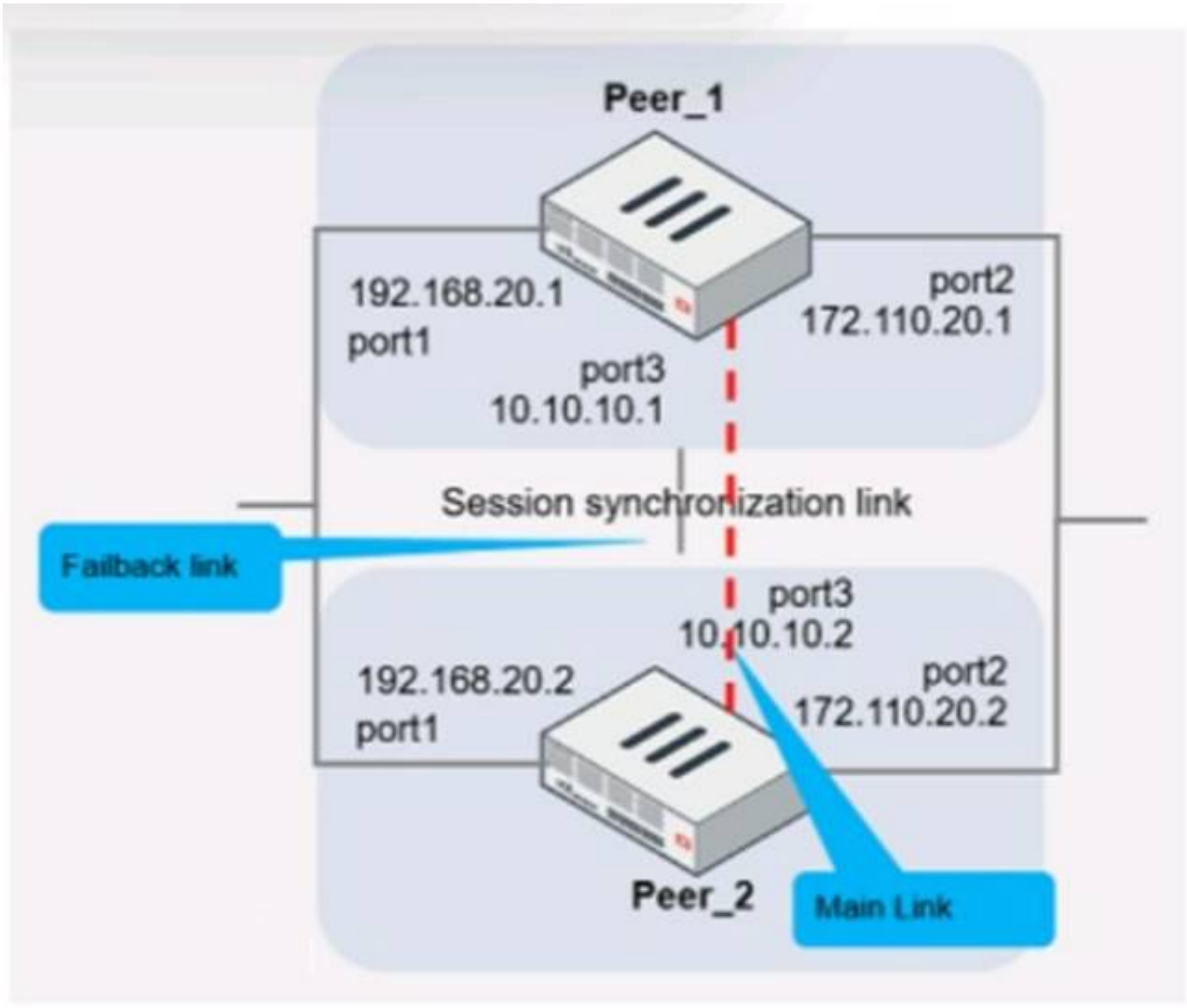
Why can you modify the Engineering address object, but not the Finance address object?

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 8
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 9
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.

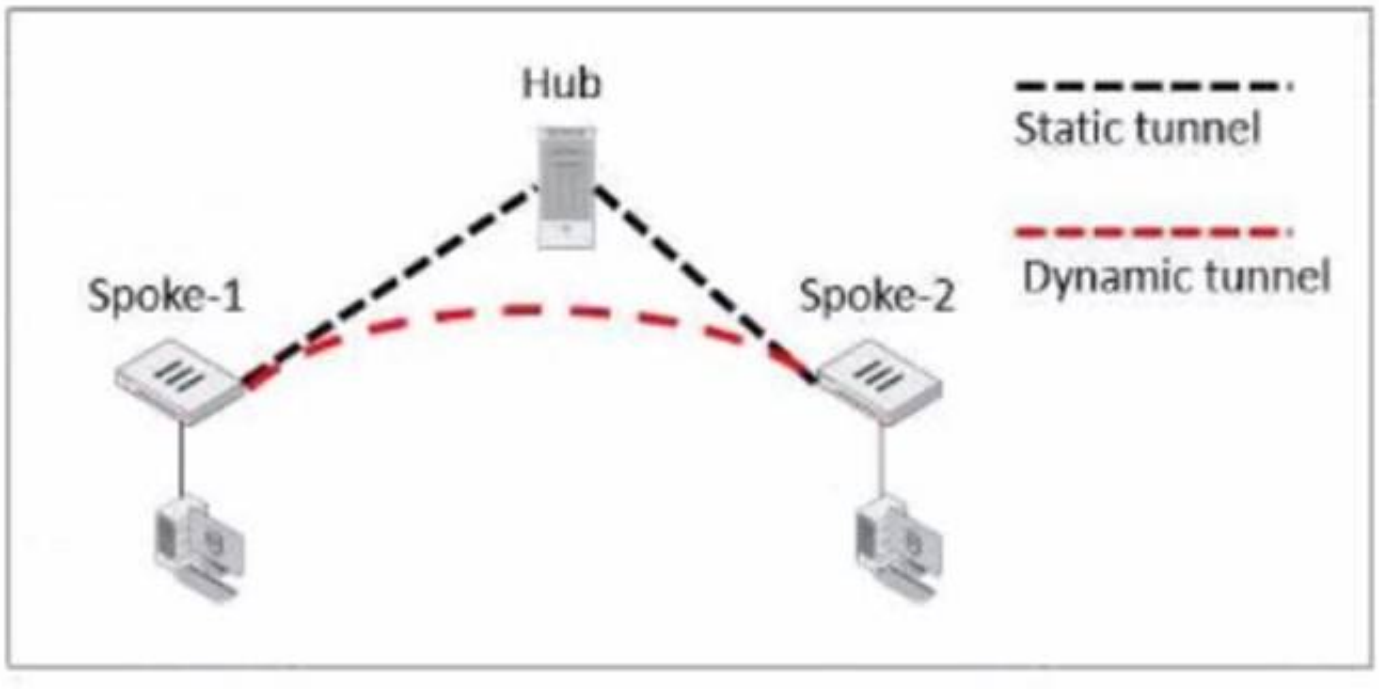
NEW QUESTION 10
Which two statements about ADVPN are true? (Choose two.)

A. You must disable add-route in the hub.
B. AllFortiGate 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 betwen spokes.

NEW QUESTION 10
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 floes the hub send to Spoke-110 bring up the dynamic tunnel?

A. Shortcut query
B. Shortcut reply
C. Shortcut offer
D. Shortcut forward

Answer: A

Explanation:
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.

NEW QUESTION 14
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 19
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 me FortiGate interfaces andthe 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 20
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-senderenabled to send shortcut advertisement messages to the spokes. Also, the hub would need to haveauto-discovery-forwarderenabled 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. Theike-versiondoes not need to be reconfigured on the hub if it's already set to version 2 andauto-discovery-receiveris not necessary on the hub because it's the one sending the advertisements, not receiving.
References:
? FortiOS Handbook - ADVPN

NEW QUESTION 25
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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