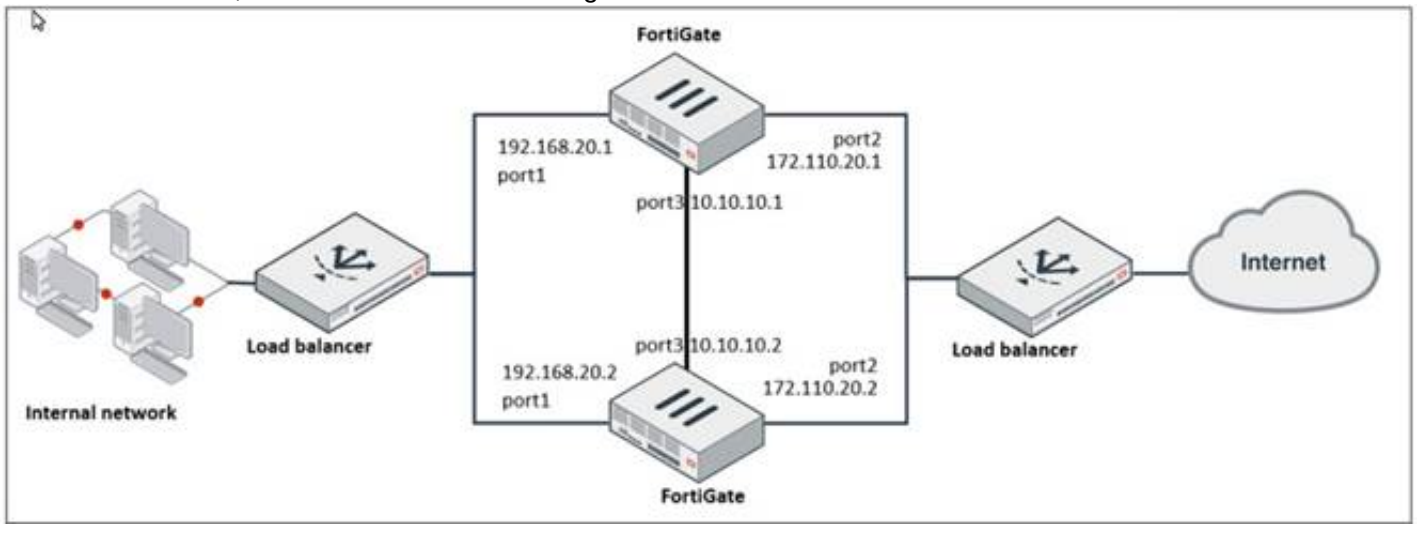
Fortinet

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”.

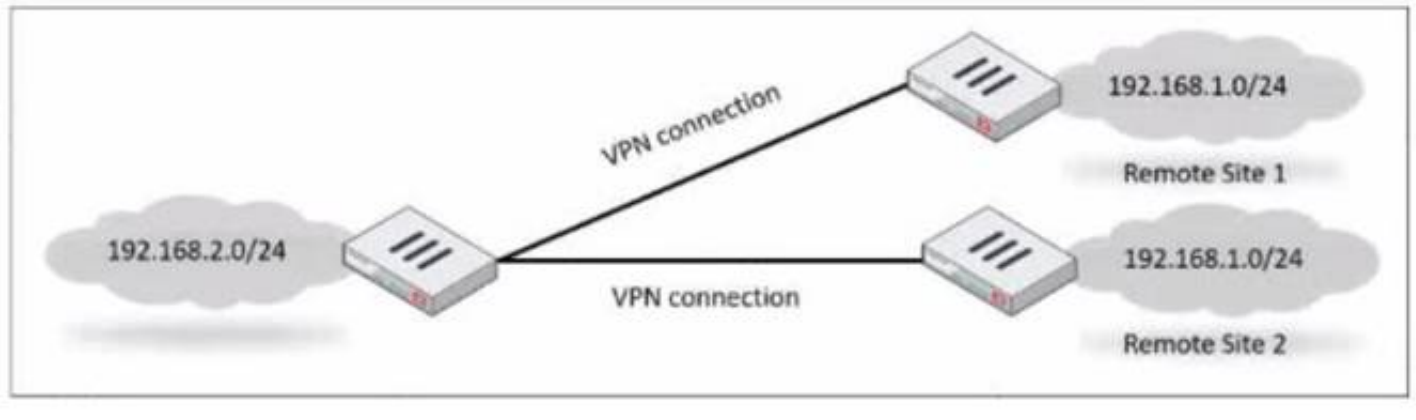
NEW QUESTION 3
Winch two statements about ADVPN are true? (Choose two)

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 4
Refer to the exhibit, which shows a network diagram.



Which IPsec phase 2 configuration should you impalement 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 useroute-overlapwith 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
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)

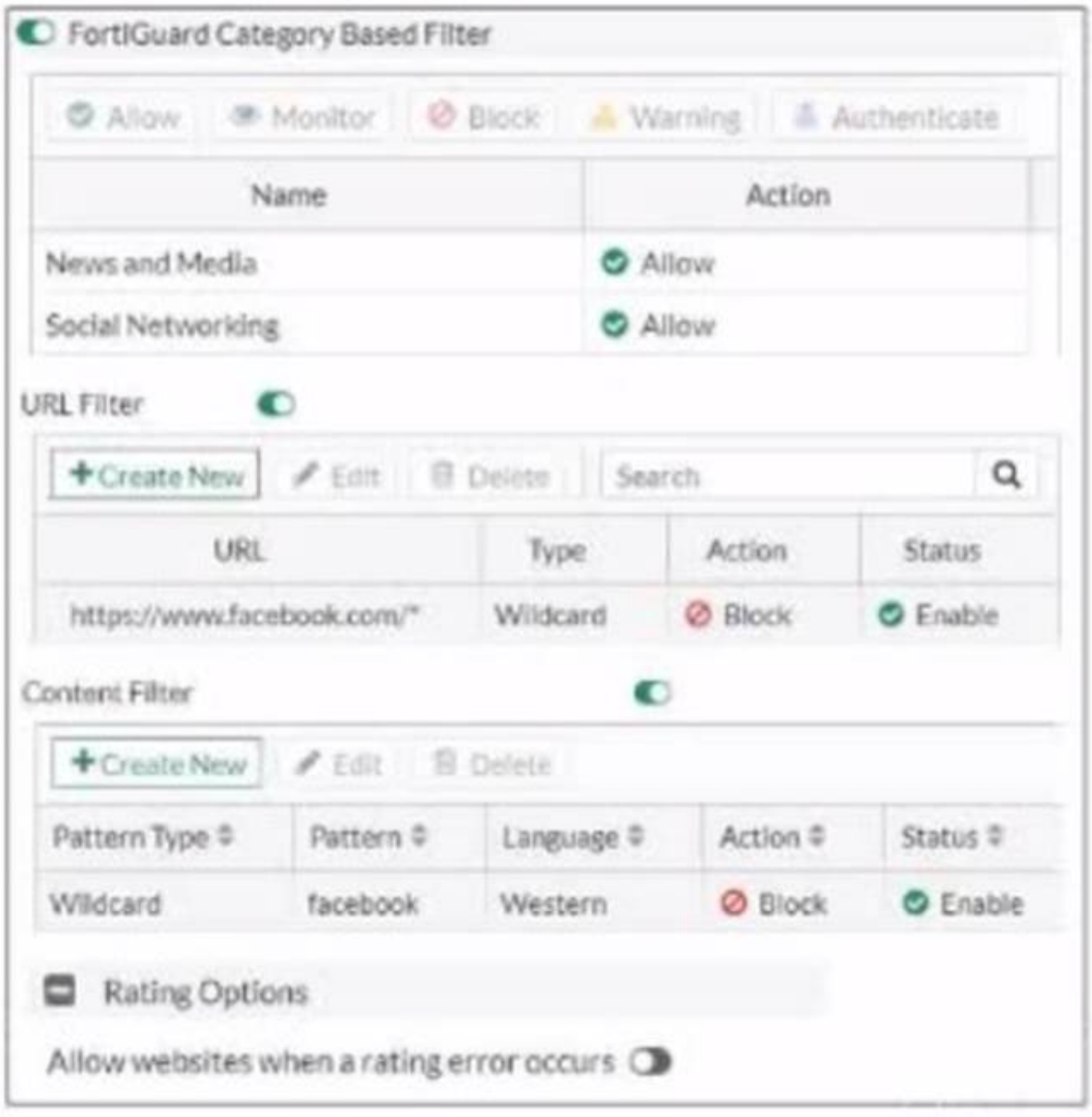
```
F-SBID( --name "eicar"; --protocol tcp; --service HTTP; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)
```

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 6
Exhibit.



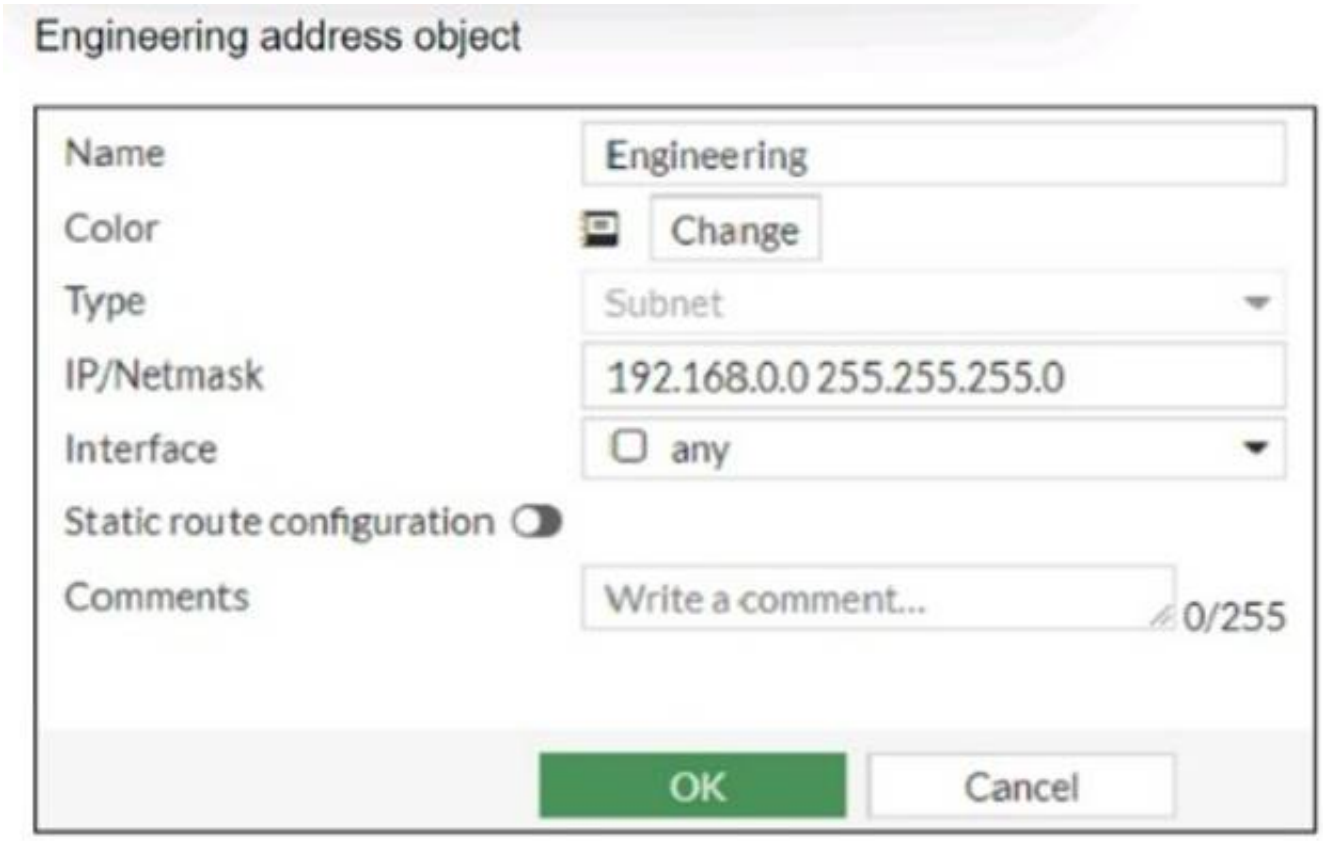
Refer to the exhibit, which shows a partial web filter profile conjuration
What can you cone udo from this configuration about access towww.facebook, com, which is categorized as Social Networking?

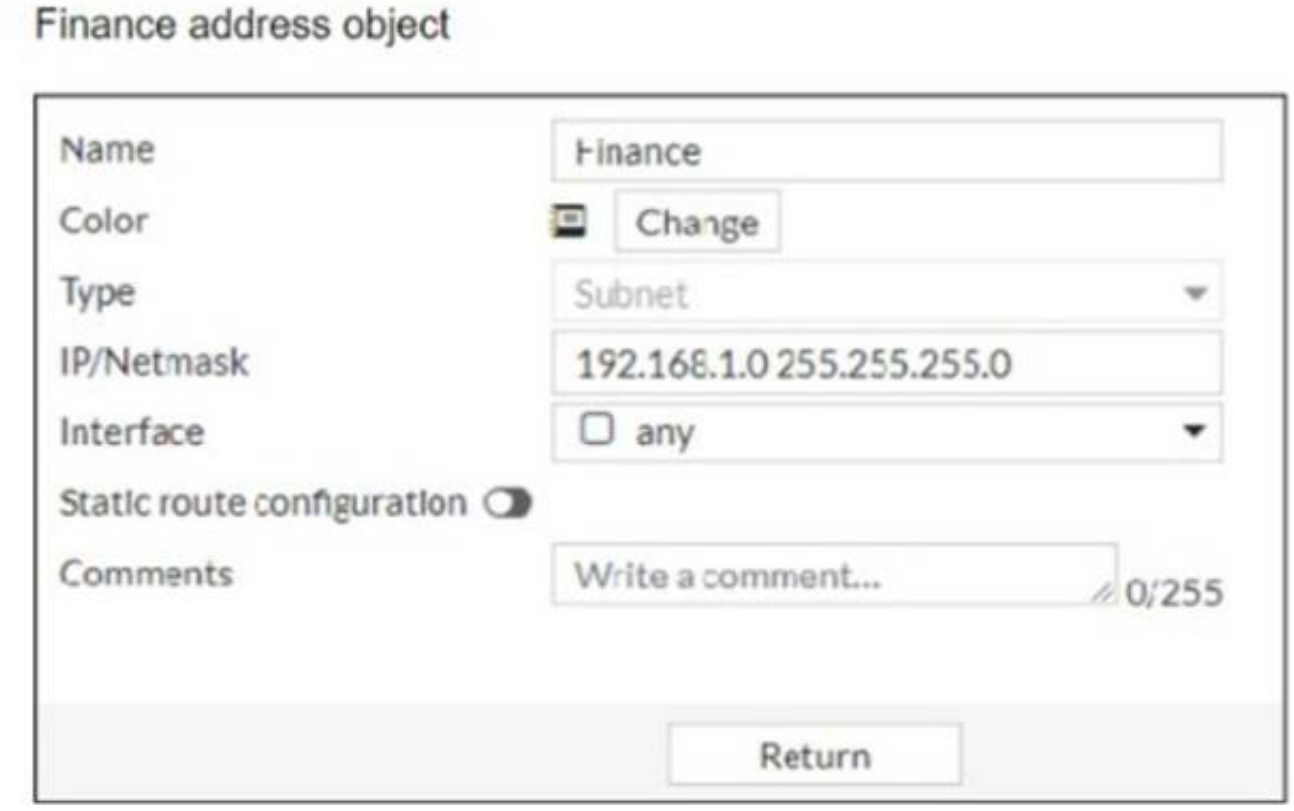
A. The access is blocked based on the Content Filter configuration
B. The access is allowed based on the FortiGuard Category Based Filter configuration
C. The access is blocked based on the URL Filter configuration
D. The access is hocked if the local or the public FortiGuard server does not reply

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 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.

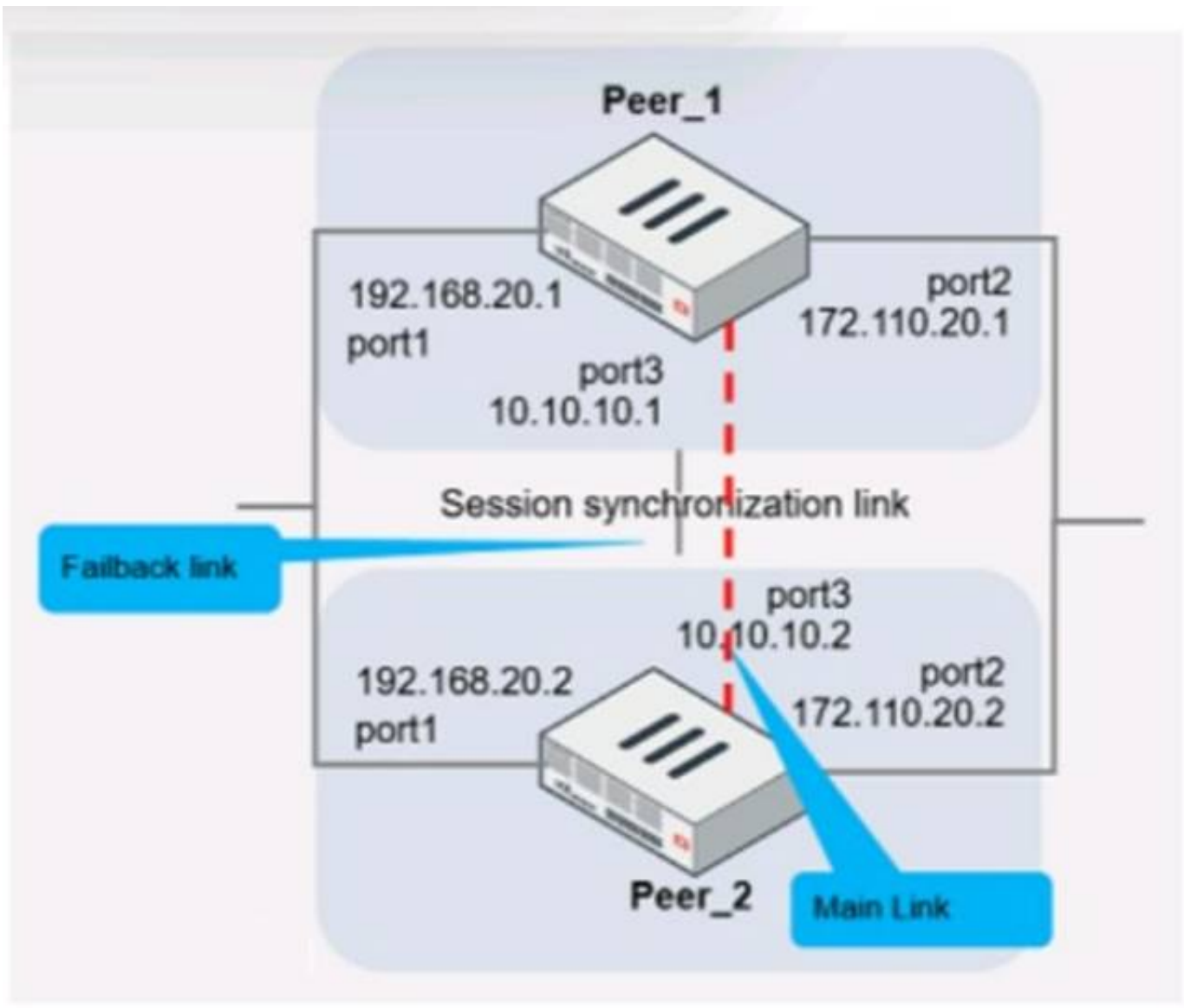
NEW QUESTION 8
Which ADVPN configuration must be configured using a script on fortiManager, when using VPN Manager to manage fortiGate VPN tunnels?

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 9
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 10
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_variabie_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 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 14
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 19
Refer to the exhibit, which shows a routing table.

Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	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	port3	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 22
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 27
In which two ways does fortiManager function when it is deployed as a local FDS? (Choose two)

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

Answer: AB

Explanation:
When deployed as a local FortiGuard Distribution Server (FDS),
FortiManager functions in several capacities. It can act as an update server, a rating server, or both, providing firmware updates and FortiGuard database updates. Additionally, it plays a crucial role in VM license validation services, ensuring that the connected FortiGate devices are operating with valid licenses. However, it does not support rating requests from non-FortiGate devices nor cache firmware updates for unmanaged devices. Fortinet FortiOS Handbook: FortiManager as a Local FDS Configuration

NEW QUESTION 30
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 32
.....

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