Fortinet

Exam Questions NSE7_EFW-7.2

Fortinet NSE 7 - Enterprise Firewall 7.2

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

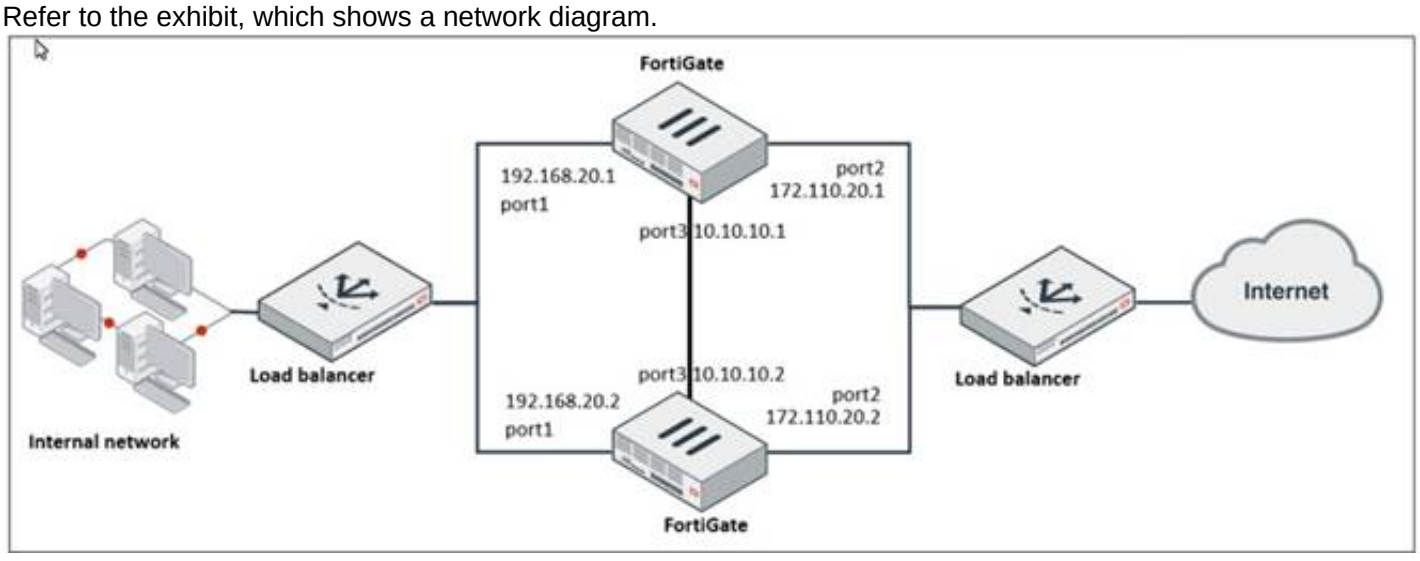
* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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 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: =

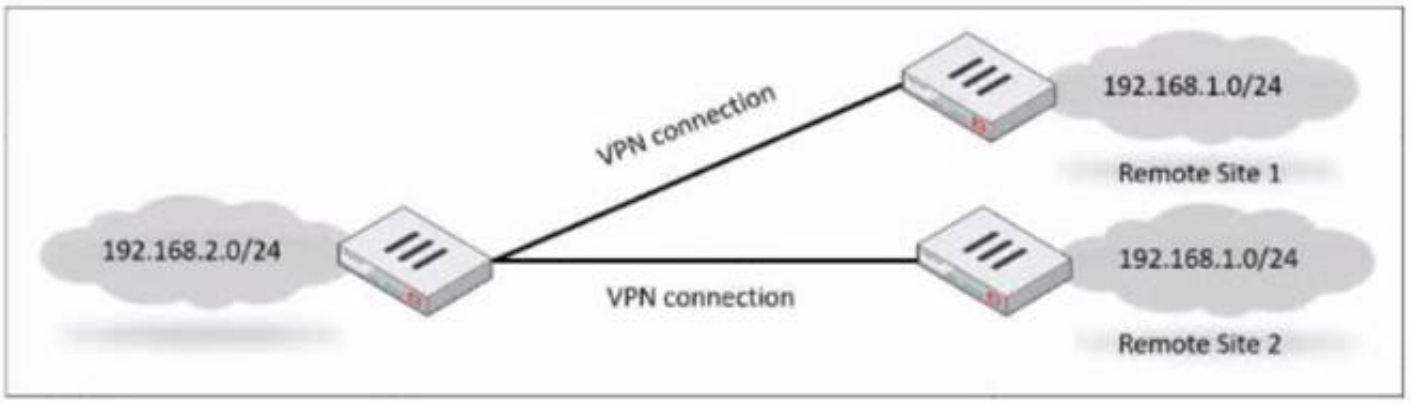
NEW QUESTION 4
Which two statements about the neighbor-group command are true? (Choose two.)

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 applyingcommon 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
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 6
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.)

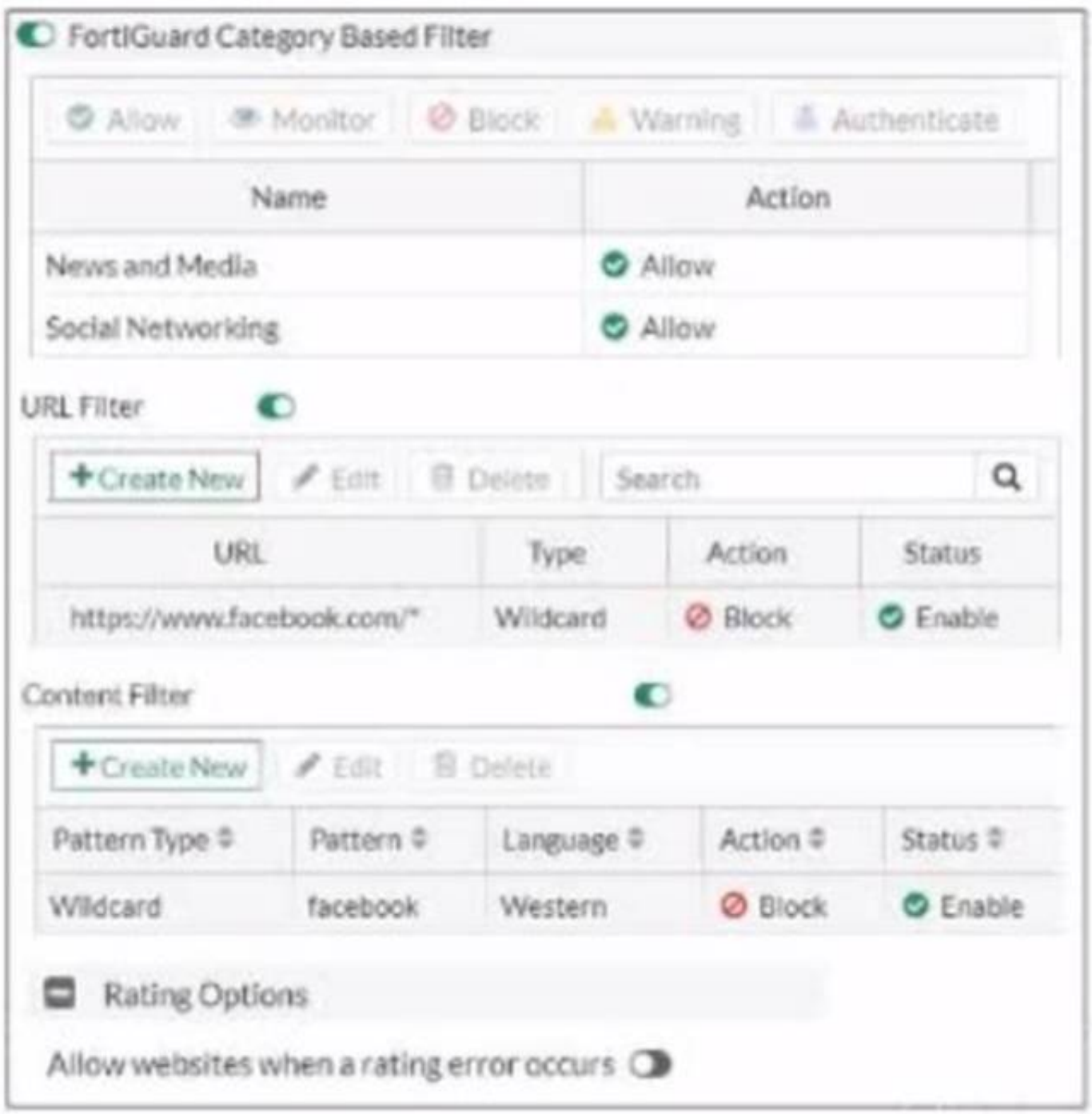
A. Dead peer detection is set to enable.
B. The IKE version is 2.

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 7
Exhibit.



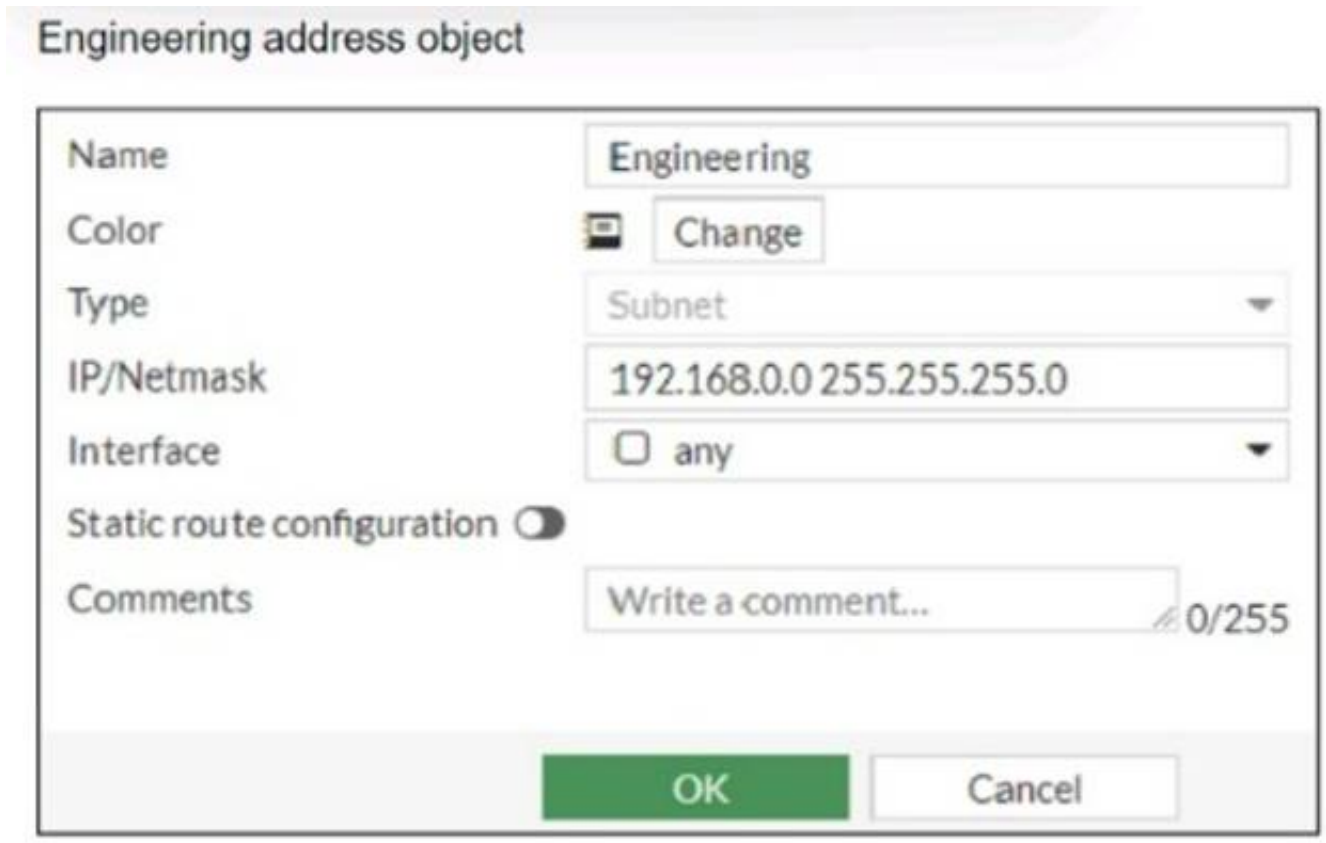
Refer to the exhibit, which shows a partial web filter profile conjuration
What can you cone udo from this configuration about access towww.facebook, com, which is categorized as Social Networking?

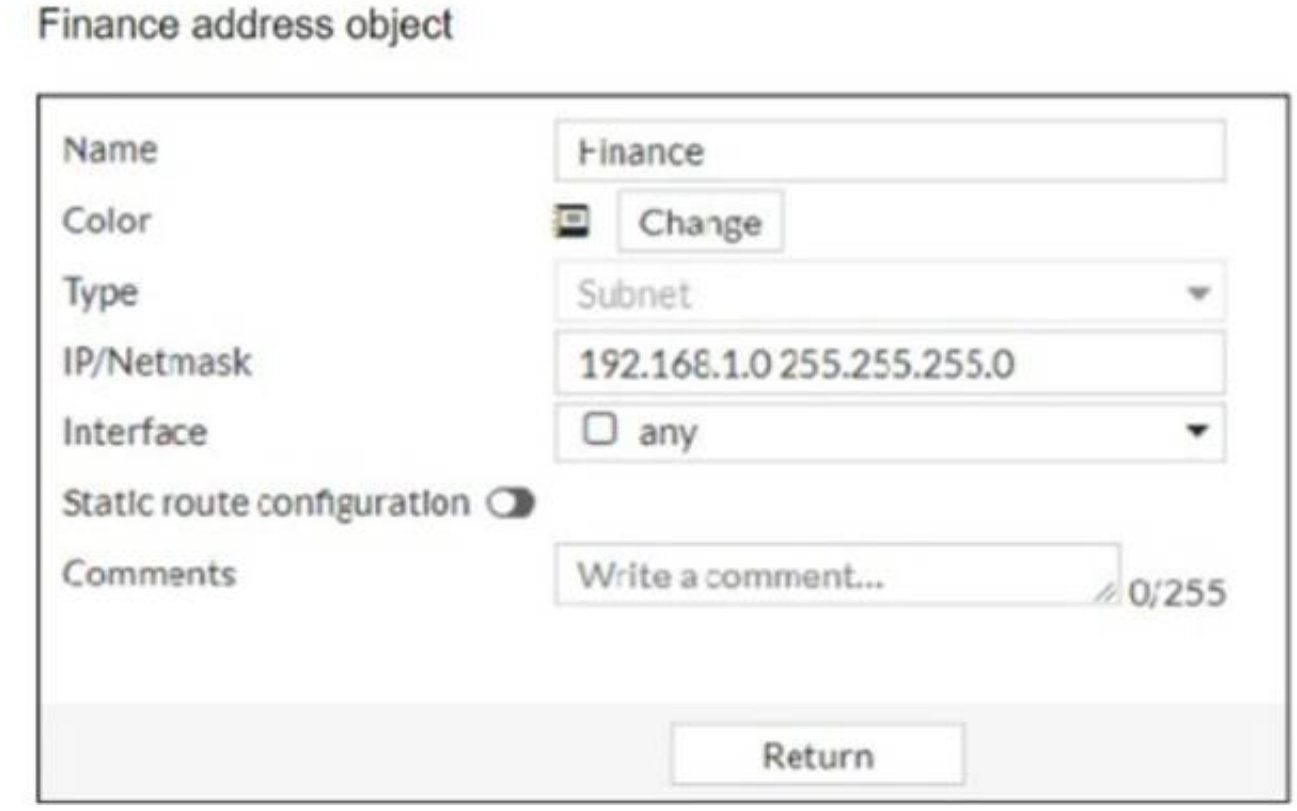
A. The access is blocked based on the Content Filter configuration
B. The access is allowed based on the FortiGuard Category Based Filter configuration
C. The access is blocked based on the URL Filter configuration
D. The access is hocked if the local or the public FortiGuard server does not reply

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 8
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.

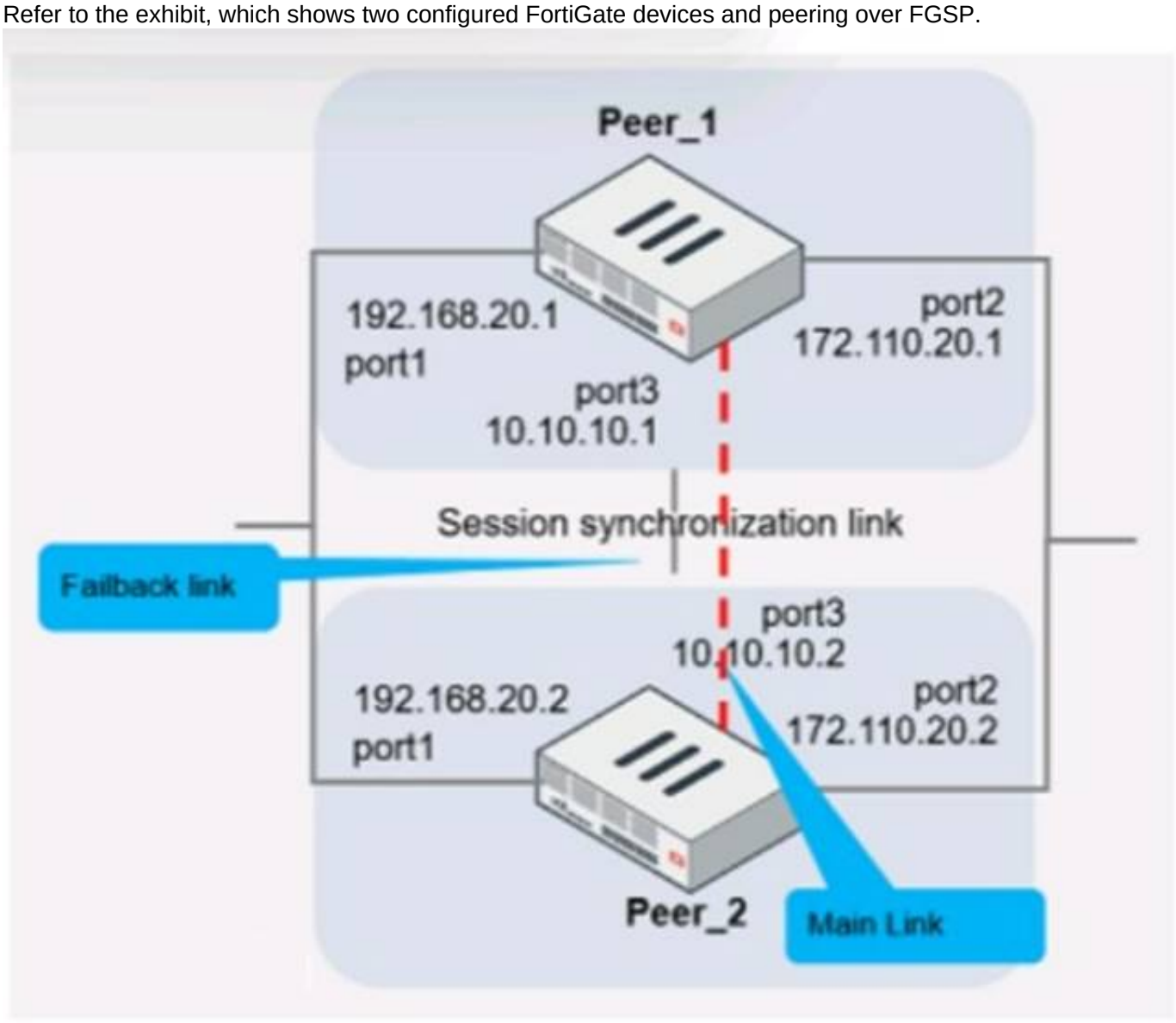
NEW QUESTION 9
You want to configure faster failure detection for BGP
Which parameter should you enable on both connected FortiGate devices?

A. Ebgp-enforce-multihop
B. bfd
C. Distribute-list-in
D. Graceful-restart

Answer: B

Explanation:
BFD (Bidirectional Forwarding Detection) is a protocol that provides fast failure detection for BGP by sending periodic messages to verify the connectivity between two peers1. BFD can be enabled on both connected FortiGate devices by using the command set bfd enable under the BGP configuration2. References: = Technical Tip :
FortiGate BFD implementation and examples …, Configure BGP | FortiGate / FortiOS 7.0.2
- Fortinet Documentation

NEW QUESTION 10
Refer to the exhibit, which shows two configured FortiGate devices and peering over FGSP.



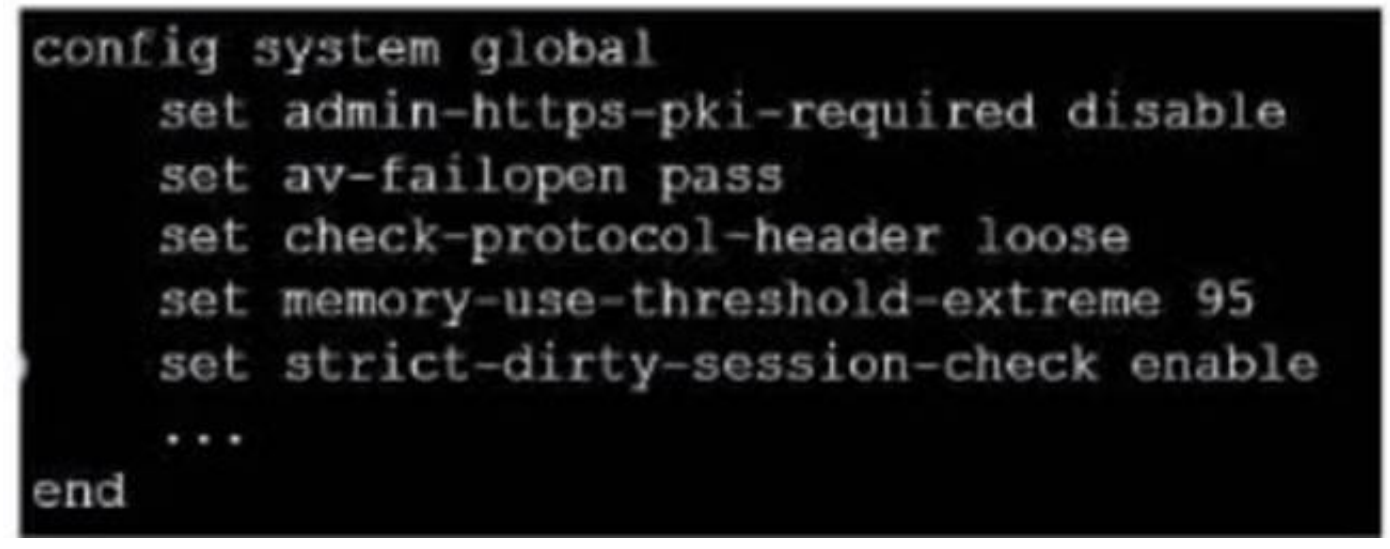
The main link directly connects the two FortiGate devices and is configured using the set session-syn-dev <interface> command.
What is the primary reason to configure the main link?

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 10
Refer to the exhibit.



which contains a partial configuration of the global system. What can you conclude from this output?

A. NPs and CPs are enabled
B. Only CPs arc disabled
C. Only NPs are disabled
D. NPs and CPs arc disabled

Answer: D

Explanation:
The configuration output shows various global settings for a FortiGate device. The terms NP (Network Processor) and CP (Content Processor) relate to FortiGate's hardware acceleration features. However, the provided configuration output does not directly mention the status (enabled or disabled) of NPs and CPs. Typically, the command to disable or enable hardware acceleration features would specifically mention NP or CP in the command syntax. Therefore, based on the output provided, we cannot conclusively determine the status of NPs and CPs, hence option D is the closest answer since the output does not confirm that they are enabled.
References:
? FortiOS Handbook - CLI Reference for FortiOS 5.2

NEW QUESTION 12
Which two statements about IKE vision 2 are true? (Choose two.)

A. Phase 1 includes main mode
B. It supports the extensible authentication protocol (EAP)
C. It supports the XAuth protocol.
D. It exchanges a minimum of four messages to establish a secure tunnel

Answer: BD

Explanation:
IKE version 2 supports the extensible authentication protocol (EAP), which allows for more flexible and secure authentication methods1. IKE version 2 also exchanges a minimum of four messages toestablish a secure tunnel, which is more efficient than IKE version 12. References: = IKE settings | FortiClient 7.2.2 - Fortinet Documentation, Technical Tip: How to configure IKE version 1 or 2 … - Fortinet Community

NEW QUESTION 16
After enabling IPS you receive feedback about traffic being dropped. What could be the reason?

A. Np-accel-mode is set to enable
B. Traffic-submit is set to disable
C. IPS is configured to monitor
D. Fail-open is set to disable

Answer: D

Explanation:
Fail-open is a feature that allows traffic to pass through the IPS sensor without inspection when the sensor fails or is overloaded. If fail-open is set to disable, traffic will be dropped in such scenarios1. References: = IPS | FortiGate / FortiOS 7.2.3 - Fortinet Documentation
When IPS (Intrusion Prevention System) is configured, iffail-openis set to disable, it means that if the IPS engine fails, traffic will not be allowed to pass through, which can result in traffic being dropped (D). This is in contrast to a fail-open setting, which would allow traffic to bypass the IPS engine if it is not operational.

NEW QUESTION 21
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 25
Which configuration can be used to reduce the number of BGP sessions in on IBGP network?

A. Route-reflector-peer enable
B. Route-reflector-client enable
C. Route-reflector enable
D. Route-reflector-server enable

Answer: B

Explanation:
To reduce the number of BGP sessions in an IBGP network, you can use a route reflector, which acts as a focal point for IBGP sessions and readvertises the prefixes to all other peers. To configure a route reflector, you need to enable the route-reflector- client option on the neighbor-group settings of the hub device. This will make the hub device act as a route reflector server and the other devices as route reflector clients. References := Route exchange | FortiGate / FortiOS 7.2.0 - Fortinet Documentation

NEW QUESTION 26
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 31
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 filler 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 34
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 36
Which FortiGate in a Security I auric sends togs to FortiAnalyzer?

A. Only the root FortiGate.
B. Each FortiGate in the Security fabric.
C. The FortiGate devices performing network address translation (NAT) or unified threat management (UTM). if configured.
D. Only the last FortiGate that handled a session in the Security Fabric

Answer: B

Explanation:
? Option B is correct because each FortiGate in the Security Fabric can send logs to FortiAnalyzer for centralized logging and analysis12. This allows you to monitor and manage the entire Security Fabric from a single console and view aggregated reports and dashboards.
? Option A is incorrect because the root FortiGate is not the only device that can send logs to FortiAnalyzer. The root FortiGate is the device that initiates the Security Fabric and acts as the central point of contact for other FortiGate devices3. However, it does not have to be the only log source for FortiAnalyzer.
? Option C is incorrect because the FortiGate devices performing NAT or UTM are not the only devices that can send logs to FortiAnalyzer. These devices can perform additional security functions on the traffic that passes through them, such as firewall, antivirus, web filtering, etc4. However, they are not the only devices that generate logs in the Security Fabric.
? Option D is incorrect because the last FortiGate that handled a session in the Security Fabric is not the only device that can send logs to FortiAnalyzer. The last FortiGate is the device that terminates the session and applies the final security policy5. However, it does not have to be the only device that reports the session information to FortiAnalyzer. References: =
? 1: Security Fabric - Fortinet Documentation1
? 2: FortiAnalyzer Demo6
? 3: Security Fabric topology
? 4: Security Fabric UTM features
? 5: Security Fabric session handling

NEW QUESTION 40
In which two ways does fortiManager function when it is deployed as a local FDS? (Choose two)

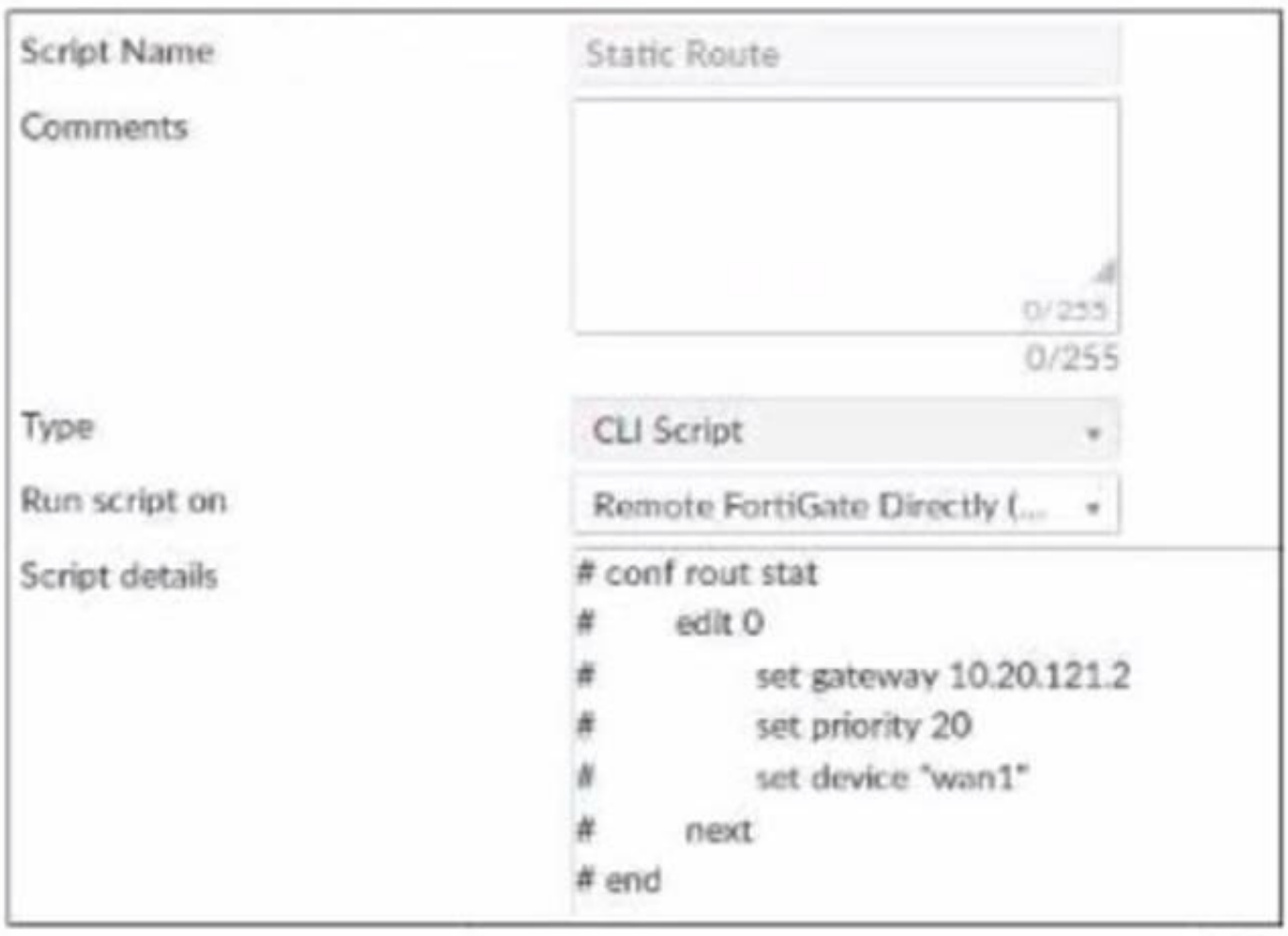
A. lt can be configured as an update server a rating server or both
B. It provides VM license validation services
C. It supports rating requests from non-FortiGate devices.
D. It caches available firmware updates for unmanaged devices

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 43
Exhibit.



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 44
You want to improve reliability over a lossy IPSec tunnel.
Which combination of IPSec phase 1 parameters should you configure?

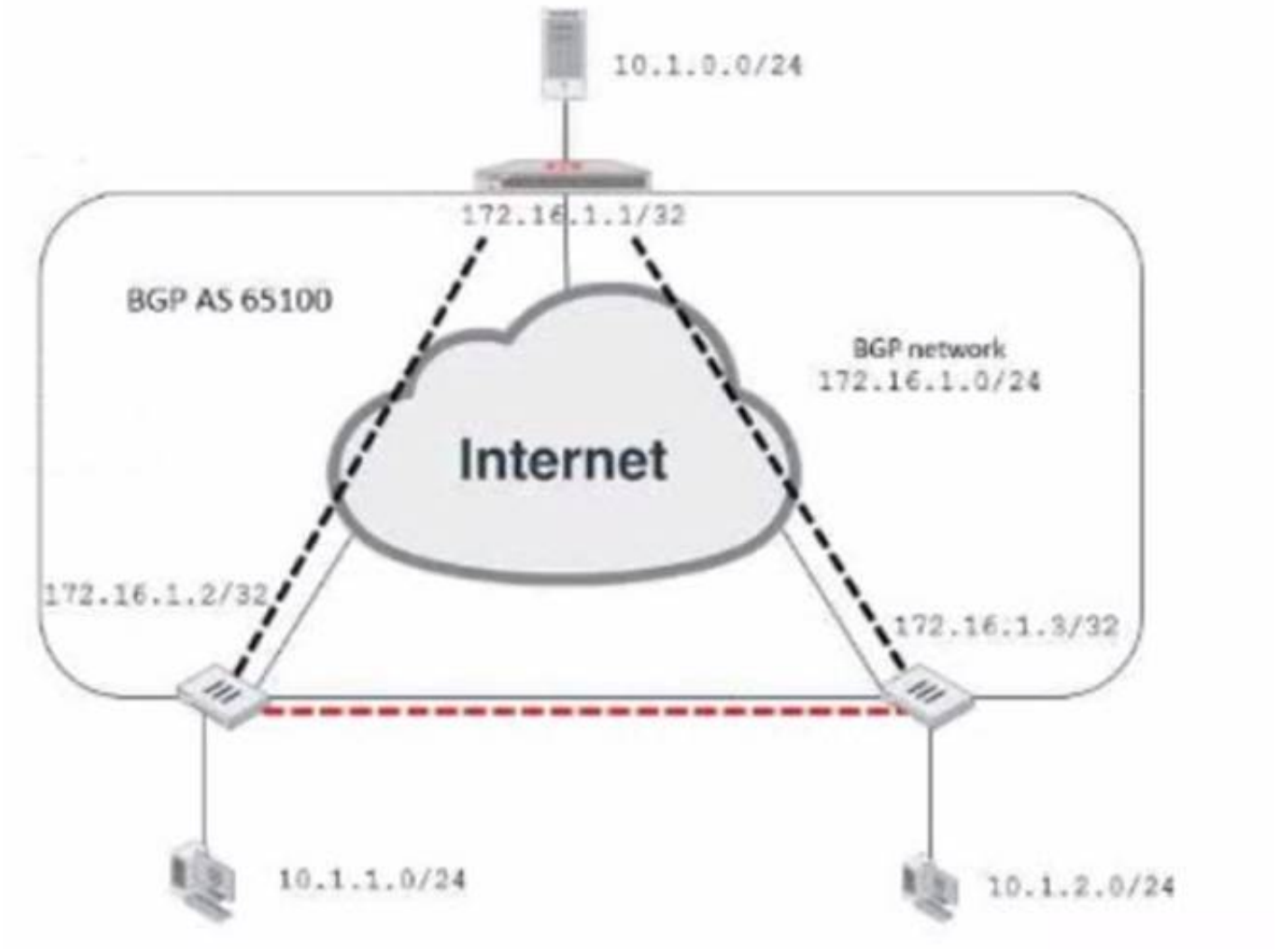
A. fec-ingress and fec-egress
B. Odpd and dpd-retryinterval
C. fragmentation and fragmentation-mtu
D. keepalive and keylive

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 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 con figuration 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 51
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 52
.....

Relate Links

100% Pass Your NSE7_EFW-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/NSE7_EFW-7.2-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/