Number: NSE7_EFW-7.2
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: NSE7_EFW-7.2

Exam Name: Fortinet NSE 7 - Enterprise Firewall 7.2

Exam A

QUESTION 1
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

Correct Answer: A
Section:
Explanation:
Option A is correct because the FortiGate CPU offloads the first packets of TCP sessions to the NP for faster connection establishment and reduced CPU load1.This feature is called TCP offloading and it is enabled by default on FortiGate models with NP6 or higher2.
Option B is incorrect because the NP does not provide IPS signature matching.The NP only handles the packet forwarding and encryption/decryption functions, while the IPS signature matching is performed by the content processor (CP) or the CPU3.
Option C is incorrect because the command to disable the NP for each firewall policy isset np-acceleration disable, notset np-acceleration st to loose4.This command can be used to prevent certain traffic types from being offloaded to the NP, such as multicast, broadcast, or non-IP packets5.
Option D is incorrect because the NP does not check the session key or IPSec SA. The NP only offloads the IPSec encryption/decryption and tunneling functions, while the session key and IPSec SA are managed by the CPU.Reference: =
1: TCP offloading
2: Network processors (NP6, NP6XLite, NP6Lite, and NP4)
3: Content processors (CP9, CP9XLite, CP9Lite)
4: Disabling NP offloading for firewall policies
5: NP hardware acceleration alters packet flow
: IPSec VPN concepts

QUESTION 2
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

Correct Answer: C
Section:
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.Reference:=Fortinet Enterprise Firewall Study Guide for FortiOS 7.2, page 132.

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.

Correct Answer: B, D
Section:
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.Reference: =
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

QUESTION 4
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

Correct Answer: A
Section:
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.Reference:=ADVPN | FortiManager 7.2.0 - Fortinet Documentation

QUESTION 5
Exhibit.

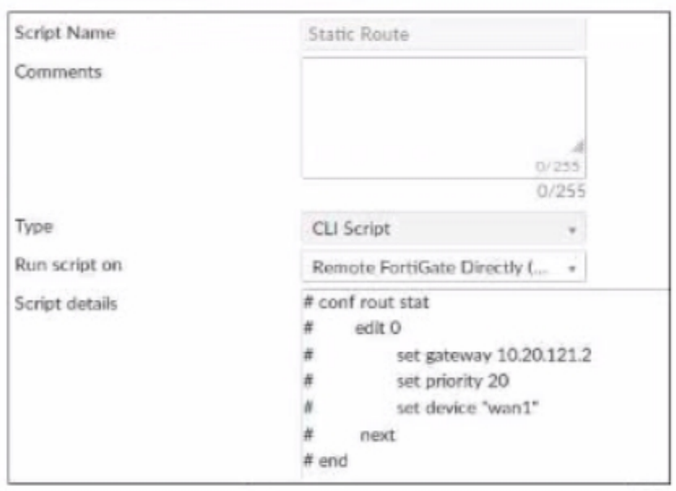
```
# get router info bgp neighbors
VRF 0 neighbor table:
BGP neighbor is 10.2.0.254, remote AS 65100, local AS 65200, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Not directly connected EBGP
  Last read 00:04:40, hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 180, keepalive interval is 60 seconds
  Received 5 messages, 0 notifications, 0 in queue
  Sent 4 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  NLRI treated as withdraw: 0
  Minimum time between advertisement runs is 30 seconds…
```

Refer to the exhibit, which provides information on BGP neighbors.
Which can you conclude from this command output?

A. The router are in the number to match the remote peer.
B. You must change the AS number to match the remote peer.
C. BGP is attempting to establish a TCP connection with the BGP peer.
D. The bfd configuration to set to enable.

Correct Answer: C
Section:
Explanation:
The BGP state is ''Idle'', indicating that BGP is attempting to establish a TCP connection with the peer. This is the first state in the BGP finite state machine, and it means that no TCP connection has been established yet. If the TCP connection fails, the BGP state will reset to either active or idle, depending on the configuration.Reference: You can find more information about BGP states and troubleshooting in the following Fortinet Enterprise Firewall 7.2 documents:
Troubleshooting BGP
How BGP works

QUESTION 6
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 #!.

Correct Answer: A, B
Section:
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 #!.Reference:=Configuring custom scripts | FortiManager 7.2.0 - Fortinet Documentation, section ''CLI script syntax''.

QUESTION 7
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)

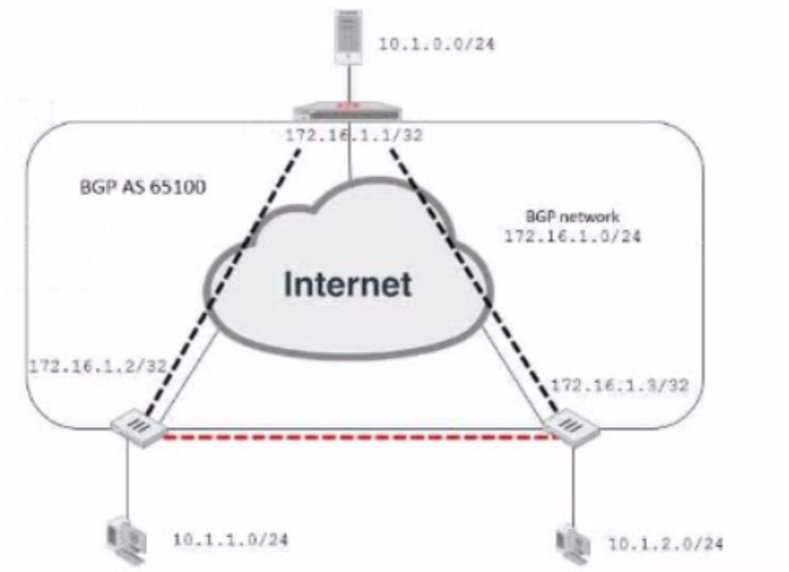
A. 10.1.5.254 is the default gateway of the internal network
B. On failover new primary device uses the same MAC address as the old primary
C. The VRRP domain uses the physical MAC address of the primary FortiGate
D. By default FortiGate B is the primary virtual router

Correct Answer: B, C
Section:
Explanation:
The configuration shows that VRRP (Virtual Router Redundancy Protocol) is enabled and both FortiGates have the vrrp-virtual-mac enable command, meaning they share the same MAC address. The primary FortiGate uses its physical MAC address as indicated by the set type physical command. The priority value determines which FortiGate is the primary virtual router, and in this case, FortiGate-A has a higher priority than FortiGate-B, so it is the

primary by default. The IP address 10.1.5.254 is the virtual IP address of the VRRP group, not the default gateway of the internal network.Reference: You can find more information about VRRP configuration and troubleshooting in the following Fortinet Enterprise Firewall 7.2 documents:
VRRP
Technical Tip: FortiGate VRRP configuration and debug
Configuration Example: How to configure VRRP between a FortiGate and a Cisco router

QUESTION 8
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

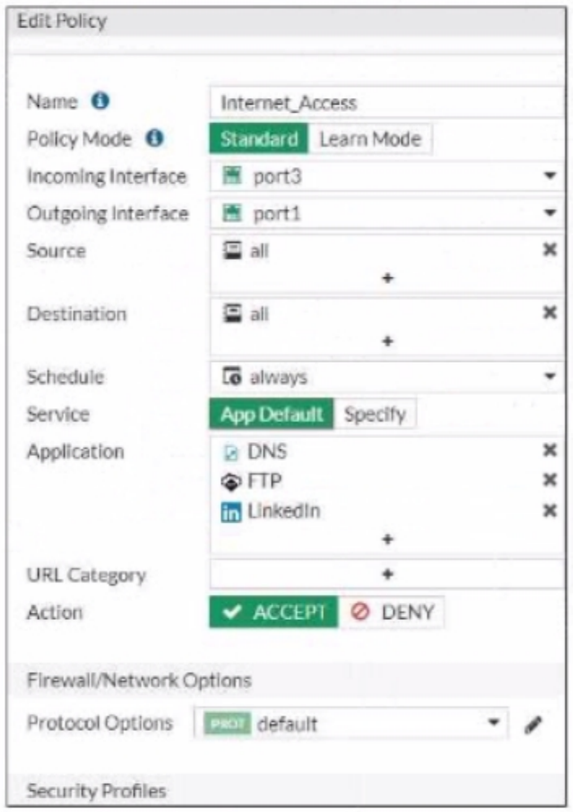
Correct Answer: C, D
Section:
Explanation:
The config neighbor range command is used to configure a range of IP addresses for BGP neighbors in an ADVPN scenario. The two parameters that should be configured are the neighbor-group and the prefix. The neighbor-group specifies the name of the neighbor group that the range belongs to, which in this case is ''advpn''. The prefix specifies the IP address range of the BGP neighbors, which in this case is 10.1.0.0/24, as shown in the network diagram.Reference: You can find more information about ADVPN and BGP configuration in the following Fortinet Enterprise Firewall 7.2 documents:
ADVPN
BGP
ADVPN with BGP as the routing protocol

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

Correct Answer: B
Section:
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 commandset bfd enableunder the BGP configuration2.Reference: =Technical Tip : FortiGate BFD implementation and examples ...,Configure BGP | FortiGate / FortiOS 7.0.2 - Fortinet Documentation

QUESTION 10
Exhibit.



Refer to the exhibit, which contains a partial policy configuration.
Which setting must you configure to allow SSH?

A. Specify SSH in the Service field
B. Configure pot 22 in the Protocol Options field.
C. Include SSH in the Application field
D. Select an application control profile corresponding to SSH in the Security Profiles section

Correct Answer: A
Section:
Explanation:
Option A is correct because to allow SSH, you need to specify SSH in the Service field of the policy configuration.This is because the Service field determines which types of traffic are allowed by the policy1. By default, the Service field is set to App Default, which means that the policy will use the default ports defined by the applications.However, SSH is not one of the default applications, so you need to specify it manually or create a custom service for it2.
Option B is incorrect because configuring port 22 in the Protocol Options field is not enough to allow SSH.The Protocol Options field allows you to customize the protocol inspection and anomaly protection settings for the policy3. However, this field does not override the Service field, which still needs to match the traffic type.
Option C is incorrect because including SSH in the Application field is not enough to allow SSH.The Application field allows you to filter the traffic based on the application signatures and categories4. However, this field does not override the Service field, which still needs to match the traffic type.
Option D is incorrect because selecting an application control profile corresponding to SSH in the Security Profiles section is not enough to allow SSH. The Security Profiles section allows you to apply various security features to the traffic, such as antivirus, web filtering, IPS, etc. However, this section does not override the Service field, which still needs to match the traffic type.Reference: =
1: Firewall policies
2: Services
3: Protocol options profiles

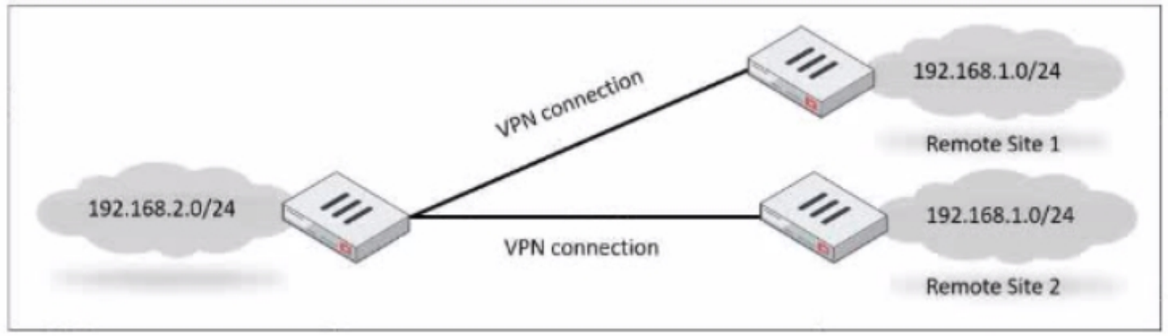
4: Application control

QUESTION 11
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

Correct Answer: B, D
Section:
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 to establish a secure tunnel, which is more efficient than IKE version 12.Reference: =IKE settings | FortiClient 7.2.2 - Fortinet Documentation,Technical Tip: How to configure IKE version 1 or 2 ... - Fortinet Community

QUESTION 12
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

Correct Answer: B
Section:
Explanation:
The ''single-source'' option ensures that only one remote site is connected at any time, which aligns with the requirement in the question. This option prevents multiple VPN tunnels from being established between the same source and destination networks, and allows only the most recent tunnel to be active. This can be useful for scenarios where multiple remote sites have the same IP address range, as shown in the exhibit.Reference:=Fortinet Enterprise Firewall Study Guide for FortiOS 7.2, page 142.

QUESTION 13
You contoured an address object on the tool fortiGate in a Security Fabric. This object is not synchronized with a downstream device. Which two reasons could be the cause? (Choose two)

A. The address object on the tool FortiGate has fabric-object set to disable
B. The root FortiGate has configuration-sync set to enable

C. The downstream TortiGate has fabric-object-unification set to local
D. The downstream FortiGate has configuration-sync set to local

Correct Answer: A, C
Section:
Explanation:
Option A is correct because the address object on the tool FortiGate will not be synchronized with the downstream devices if it has fabric-object set to disable.This option controls whether the address object is shared with other FortiGate devices in the Security Fabric or not1.
Option C is correct because the downstream FortiGate will not receive the address object from the tool FortiGate if it has fabric-object-unification set to local.This option controls whether the downstream FortiGate uses the address objects from the root FortiGate or its own local address objects2.
Option B is incorrect because the root FortiGate has configuration-sync set to enable by default, which means that it will synchronize the address objects with the downstream devices unless they are disabled by the fabric-object option3.
Option D is incorrect because the downstream FortiGate has configuration-sync set to local by default, which means that it will receive the address objects from the root FortiGate unless they are overridden by the fabric-object-unification option4.Reference: =
1: Group address objects synchronized from FortiManager5
2: Security Fabric address object unification6
3: Configuration synchronization7
4: Configuration synchronization7
: Security Fabric - Fortinet Documentation

QUESTION 14
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

Correct Answer: B, D
Section:
Explanation:
Metadata variables are custom fields that you can create on FortiManager to store additional information about objects or devices. They can be used as variables in Jinja2 CLI templates or scripts to apply configurations to multiple devices or objects. They do not apply only to non-firewall objects, but also to firewall objects such as addresses, services, policies, etc. The metadata format is not $<metadata_variable_name>, but @<metadata_variable_name>@.Reference:=Using meta field variables,Metadata Variables are supported in Firewall Objects configuration,Technical Tip: New Meta Variables and their usage including Jinja Templates,Technical Tip: Firewall objects use as metadata variable

QUESTION 15
Refer to the exhibit, which contains a partial BGP combination.

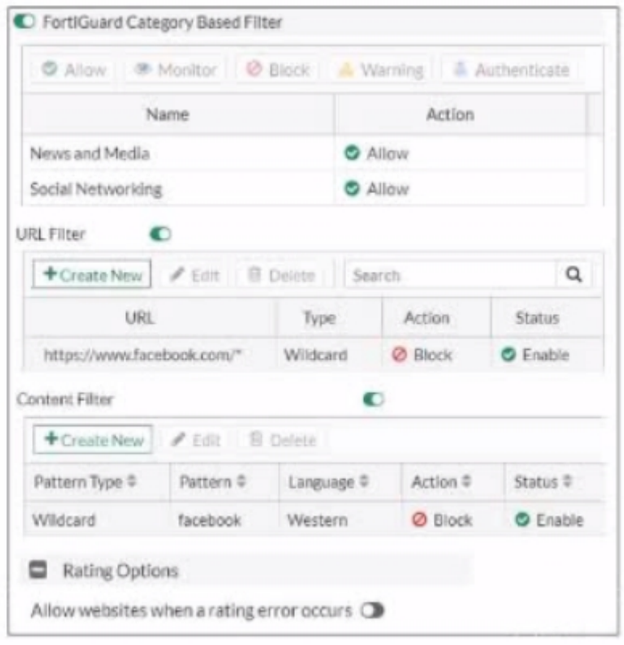
```
config router bgp
    set as 65200
    set router-id 172.16.1.254
    config neighbor
        edit 100.64.1.254
            set remote-as 65100
        next
    end
end
```

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

Correct Answer: A, D
Section:
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.Reference:=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

QUESTION 16
Exhibit.



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

Correct Answer: C
Section:
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.Reference:=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

QUESTION 17
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. Verity Mai the speed and duplex settings match between me FortiGate interfaces and the connected switch ports
B. Configure set link -failed signal enable under-config system ha on both Cluster members
C. Configure remote Iink 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

Correct Answer: B
Section:
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.

QUESTION 18
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

Correct Answer: A, D
Section:

QUESTION 19
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

Correct Answer: A, D
Section:
Explanation:
The command output shows that the Neighbor Count is 2, indicating that there are more than one OSPF routers on the port3 network (Option A). NGFW-1 is also identified as the Designated Router (Option D).Reference:=OSPF | FortiGate / FortiOS 7.2.2 - Fortinet Documentation,OSPF configuration guide for ABR ... - Fortinet ... - Fortinet Community

QUESTION 20
Refer to the exhibit.

```
config system global
    set admin-https-pki-required disable
    set av-failopen pass
    set check-protocol-header loose
    set memory-use-threshold-extreme 95
    set strict-dirty-session-check enable
    ...
end
```

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

Correct Answer: A
Section:
Explanation:
The configuration does not show any explicit disabling of NPs (Network Processors) or CPs (Content Processors).In Fortinet Enterprise Firewall, unless explicitly disabled, these processors are enabled by default to handle specific types of traffic efficiently12.Reference:=Hardware acceleration | FortiGate / FortiOS 7.2.2 - Fortinet Documentation,NSE 7 Network Security Architect - Fortinet