Free Questions for NSE7_NST-7.2

Shared by Morris on 04-10-2024

For More Free Questions and Preparation Resources

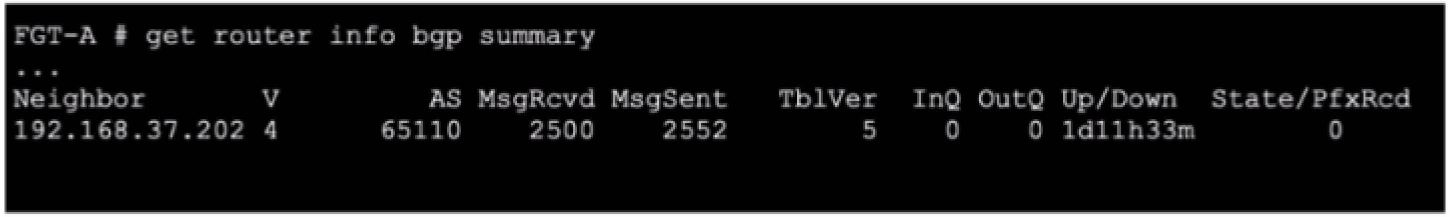
Check the Links on Last Page

Question 1

Question Type: MultipleChoice

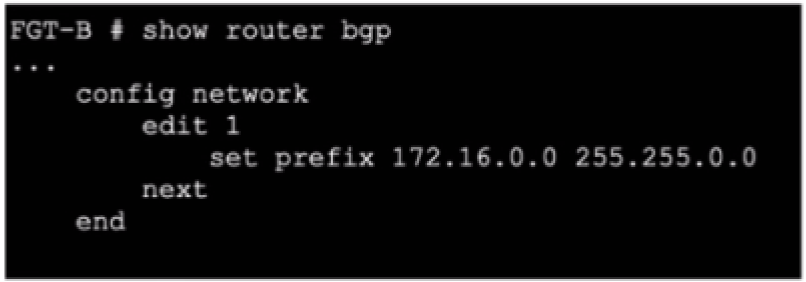
Refer to the exhibits.

Exhibit 1



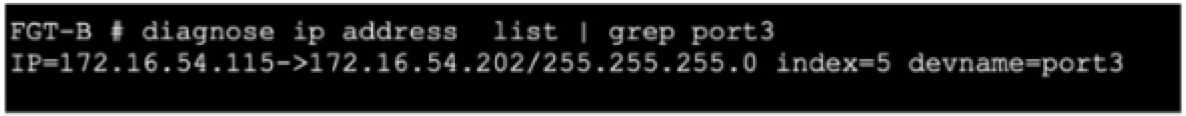
```
FGT-A # get router info bgp summary
...
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.37.202 4       65110    2500    2552        5    0    0 1d11h33m            0
```

Exhibit 2



```
FGT-B # show router bgp
...
    config network
        edit 1
            set prefix 172.16.0.0 255.255.0.0
        next
    end
```

Exhibit 3



```
FGT-B # diagnose ip address  list | grep port3
IP=172.16.54.115->172.16.54.202/255.255.255.0 index=5 devname=port3
```

An administrator is attempting to advertise the network configured on port3. However, FGT-A is not receiving the prefix.

Which two actions can the administrator take to fix this problem" (Choose two.)

Options:

A- Restart BGP using a soft reset, which forces both peers to exchange their complete BGP routing tables.

B- Manually add the BGP route on FGT-A.

C- Modify the prefix using the network command from 172.16.0.0/16 to 172.16.54.0724.

D- Use the set network-import-check disable command.

Answer:

A, D

Explanation:

Soft Reset of BGP:

Performing a soft reset of BGP is a common method to resolve issues where prefixes are not being received. It forces both BGP peers to resend their complete routing tables to each other.

This can be done using the command: execute router clear bgp soft in and execute router clear bgp soft out.

Network Import Check:

The network-import-check command controls whether the FortiGate should verify that the prefix exists in the routing table before advertising it.

Disabling this check can resolve issues where valid prefixes are not advertised due to stringent verification.

The command to disable this is: config router bgp set network-import-check disable end.

BGP Configuration Verification:

Ensure that the BGP configuration on FGT-B is correctly set to advertise the network 172.16.54.0/24.

Verify that the network statement is correctly configured and matches the intended prefix.

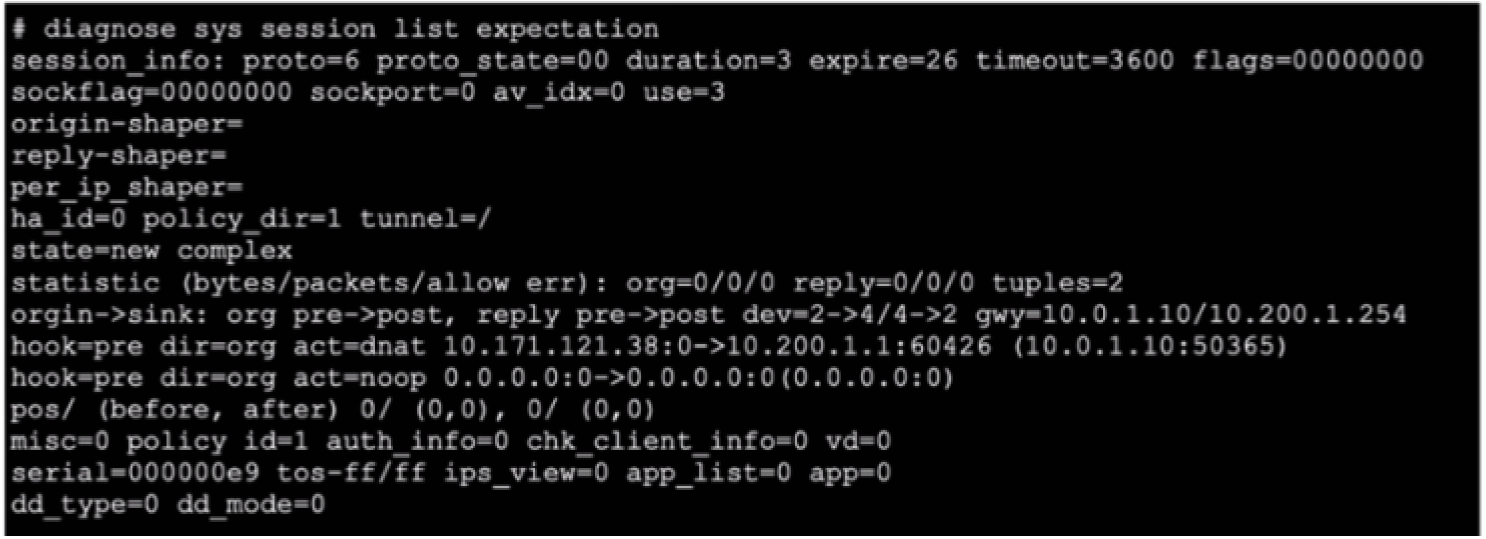
Fortinet Community: Technical Note on Configuring BGP (Welcome to the Fortinet Community!).

Fortinet Documentation: Configuring BGP on FortiGate (Fortinet Document Library).

Question 2

Question Type: **MultipleChoice**

Refer to the exhibit, which shows the output of a diagnose command



```
# diagnose sys session list expectation
session_info: proto=6 proto_state=00 duration=3 expire=26 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=1 tunnel=/
state=new complex
statistic (bytes/packets/allow err): org=0/0/0 reply=0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=2->4/4->2 gwy=10.0.1.10/10.200.1.254
hook=pre dir=org act=dnat 10.171.121.38:0->10.200.1.1:60426 (10.0.1.10:50365)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/ (before, after) 0/ (0,0), 0/ (0,0)
misc=0 policy id=1 auth_info=0 chk_client_info=0 vd=0
serial=000000e9 tos-ff/ff ips_view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

What two conclusions can you draw from the output shown in the exhibit? (Choose two.)

Options:

A- This is an expected session created by the IPS engine.

B- Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.0.1.10.

C- Traffic in the original direction (coming from the IP address 10.171.121.38) will be routed to the next-hop IP address 10.200.1.1.

D- This is a pinhole session created to allow traffic for a protocol that requires additional sessions to operate through FortiGate.

Answer:

B, D

Explanation:

Session Creation: The output shows an expected session, likely due to a pinhole, which is a dynamically created rule to allow specific traffic through the firewall.

Routing Decision:

The original direction of traffic comes from the IP address 10.171.121.38.

The next-hop IP address for this traffic is 10.0.1.10 as indicated by the routing decision in the output.

Pinhole Session: Pinhole sessions are typically created for protocols that require additional sessions (e.g., FTP, SIP) to function properly. This ensures the necessary traffic can pass through the firewall.

Debugging Commands: The diagnose sys session list command is used to list session information, which helps in understanding traffic flow and troubleshooting connectivity issues.

Fortinet Network Security Support Engineer Study Guide for FortiOS 7.2 (ebin.pub).

General IPsec VPN configuration from Fortinet documentation (Fortinet Docs).

Question 3

Question Type: **MultipleChoice**

Which statement about IKE and IKE NAT-T is true?

Options:

A- IKE is used to encapsulate ESP traffic in some situations, and IKE NAT-T is used only when the local FortiGate is using NAT on the IPsec interface.

B- IKE is the standard implementation for IKEv1 and IKE NAT-T is an extension added in IKEv2.

C- They each use their own IP protocol number.

D- They both use UDP as their transport protocol and the port number is configurable.

Answer:

D

Explanation:

IKE (Internet Key Exchange): IKE is a protocol used to set up a security association (SA) in the IPsec protocol suite. It is utilized to negotiate, create, and manage SAs.

NAT-T (Network Address Translation-Traversal): NAT-T is used to enable IPsec VPN traffic to pass through NAT devices. It encapsulates IPsec ESP packets into UDP packets.

Transport Protocol: Both IKE and IKE NAT-T use UDP as their transport protocol.

Port Numbers: By default, IKE uses UDP port 500. NAT-T typically uses UDP port 4500. However, these port numbers can be configured as needed.

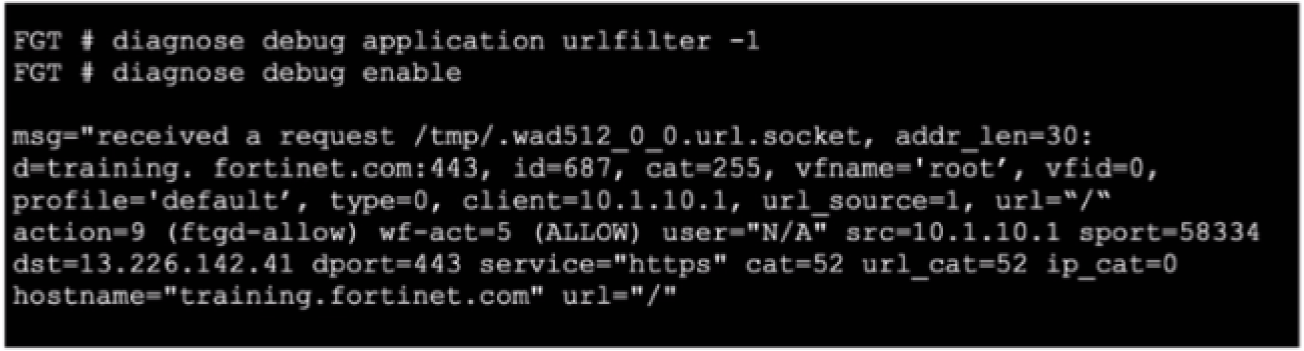
Fortinet Network Security Support Engineer Study Guide for FortiOS 7.2 (Fortinet Docs) (ebin.pub).

Fortinet Documentation on IPsec VPN Configuration (Fortinet Docs).

Question 4

Question Type: **MultipleChoice**

Refer to the exhibit, which shows the output of a real-time debug.



```
FGT # diagnose debug application urlfilter -1
FGT # diagnose debug enable

msg="received a request /tmp/.wad512_0_0.url.socket, addr_len=30:
d=training. fortinet.com:443, id=687, cat=255, vfname='root’, vfid=0,
profile='default’, type=0, client=10.1.10.1, url_source=1, url=“/“
action=9 (ftgd-allow) wf-act=5 (ALLOW) user="N/A" src=10.1.10.1 sport=58334
dst=13.226.142.41 dport=443 service="https" cat=52 url_cat=52 ip_cat=0
hostname="training.fortinet.com" url="/"
```

Which statement about this output is true?

Options:

A- The server hostname was extracted from the SNI in the client request, or from the CN in the server certificate

B- FortiGate found the requested URL in its local cache.

C- This web request was inspected using the rtgd-allow web filter profile.

D- The requested URL belongs to category ID 255.

Answer:

A

Explanation:

The exhibit displays the output of a real-time debug of the URL filtering process on a FortiGate device. The debug output includes various details about a web request being processed.

SNI (Server Name Indication): This is part of the SSL/TLS handshake where the client specifies the hostname it is trying to connect to. FortiGate can use this information to apply appropriate web filtering rules based on the server name.

CN (Common Name): This is a field in the server's SSL certificate that typically contains the server's hostname. FortiGate can extract this information to verify the identity of the server and apply security policies accordingly.

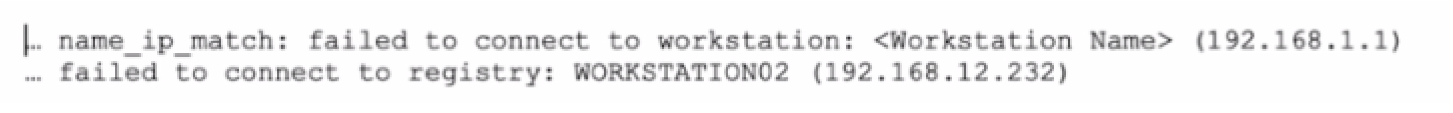
Given that the debug output includes the hostname 'training.fortinet.com,' it is likely derived from the SNI in the client's request or the CN in the server's certificate, indicating that FortiGate is using this information to process the web request.

Fortinet Community Documentation on Real-time Debugging

Question 5

Question Type: MultipleChoice

Refer to the exhibit, which shows two entries that were generated in the FSSO collector agent logs.



```
… name_ip_match: failed to connect to workstation: <Workstation Name> (192.168.1.1)
… failed to connect to registry: WORKSTATION02 (192.168.12.232)
```

What three conclusions can you draw from these log entries? (Choose three.)

Options:

A- Remote registry is not running on the workstation.

B- The FortiGate firmware version is not compatible with that of the collector agent

C- DNS resolution is unable to resolve the workstation name.

D- The user's status shows as 'not verified' in the collector agent

E- A firewall is blocking traffic to port 139 and 445.

Answer:

A, C, E

Explanation:

The exhibit shows log entries from the FSSO (Fortinet Single Sign-On) collector agent logs. These logs provide insights into why there might be issues with the collector agent connecting to workstations or the registry.

Remote registry is not running on the workstation: The failure to connect to the workstation registry can occur if the remote registry service on the workstation is not running. This service needs to be active to allow the FSSO collector agent to query the workstation for user login information.

DNS resolution is unable to resolve the workstation name: The logs indicate a failure in connecting to a workstation by name, which can happen if the DNS server is unable to resolve the workstation's name to an IP address. This is a common issue when the DNS settings are incorrect or the workstation name is not properly registered in the DNS.

A firewall is blocking traffic to port 139 and 445: Communication issues to the workstation or registry are often caused by firewall rules blocking essential ports. Ports 139 (NetBIOS) and 445 (SMB) are critical for these operations. Ensure these ports are open on both the workstation and any intermediate firewalls.

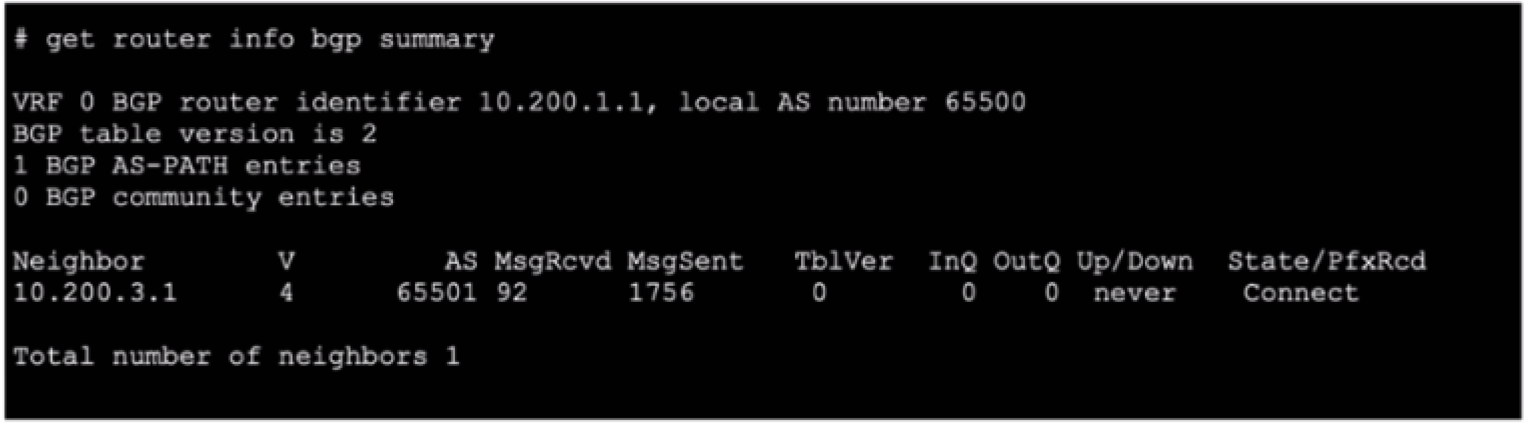
Fortinet Community Documentation on FSSO Troubleshooting

Fortinet Community on FSSO Collector Agent Issues

Question 6

Question Type: MultipleChoice

Refer to the exhibit, which shows the output of a BGP debug command.



```
# get router info bgp summary

VRF 0 BGP router identifier 10.200.1.1, local AS number 65500
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.200.3.1      4      65501 92      1756        0       0    0  never    Connect

Total number of neighbors 1
```

Which statement explains why the state of the 10.200.3.1 peer is Connect?

Options:

A- The local router initiated the BGP session to 10.200.3.1 but did not receive a response.

B- The local router is receiving BGP keepalives from the remote peer, but the local peer has not received the OpenConf inn yet.

C- The router 10.200.3.1 has authentication configured for BGP and the local router does not.

D- The local router has a different AS number than the remote peer.

Answer:

A

Explanation:

The BGP summary output shows the state of the 10.200.3.1 peer as 'Connect.' This state indicates that the local router has attempted to initiate a BGP session with the peer, but the peer has not yet responded to the initial connection request.

State Explanation: The 'Connect' state in BGP indicates that the TCP connection has been initiated but is waiting for a response. If the peer does not respond within the configured timers, the session will transition to the 'Active' state and retry the connection.

Possible Causes: This can occur due to network issues preventing the peer from responding, a misconfiguration on the peer device, or issues like access control lists (ACLs) blocking the BGP traffic.

To troubleshoot, check the connectivity between the routers, ensure that the BGP configurations on both sides match, and verify that there are no firewalls or ACLs blocking the BGP packets.

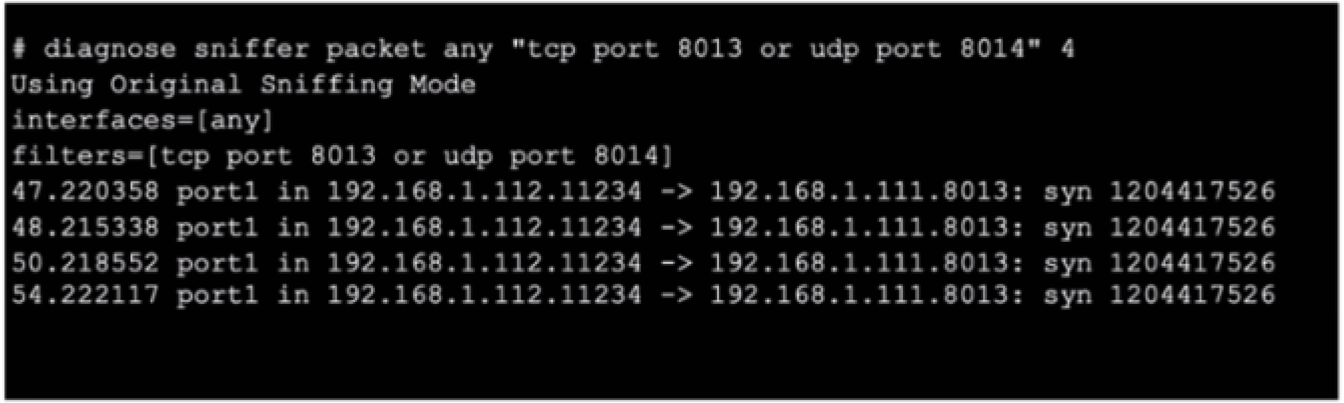
Fortinet Documentation on BGP Troubleshooting

Fortinet Community Discussion on BGP State Issues

Question 7

Question Type: MultipleChoice

Refer to the exhibit, which shows oneway communication of the downstream FortiGate with the upstream FortiGate within a Security Fabric.



```
# diagnose sniffer packet any "tcp port 8013 or udp port 8014" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[tcp port 8013 or udp port 8014]
47.220358 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
48.215338 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
50.218552 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
54.222117 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
```

What three actions must you take to ensure successful communication? (Choose three.)

Options:

A- Ensure the port for Neighbor Discovery has been changed.

B- FortiGate must not be in NAT mode.

C- Ensure TCP port 8013 is not blocked along the way

D- You must authorize the downstream FortiGate on the root FortiGate.

E- You must enable Security Fabric/Fortitelemetry on the receiving interface of the upstream FortiGate.

Answer:

C, D, E

Explanation:

The exhibit shows a sniffer capture where TCP port 8013 is being used for communication. The communication appears one-way, indicating potential issues with the upstream FortiGate receiving the necessary packets or being able to respond.

To ensure successful communication in a Security Fabric setup:

Ensure TCP port 8013 is not blocked along the way: Verify that no firewalls or network devices between the downstream and upstream FortiGates are blocking TCP port 8013. This port is crucial for Security Fabric communication.

Authorize the downstream FortiGate on the root FortiGate: In the Security Fabric, the root FortiGate must recognize and authorize the downstream FortiGate to allow proper communication and management.

Enable Security Fabric/Fortitelemetry on the receiving interface of the upstream FortiGate: The upstream FortiGate must have the Security Fabric or Fortitelemetry enabled on the interface that receives the communication from the downstream FortiGate. This enables proper data exchange and monitoring within the Security Fabric.

Fortinet Documentation on Security Fabric Configuration

Fortinet Community Discussion on Port Requirements

Question 8

Question Type: **MultipleChoice**

Refer to the exhibits, which show the configuration on FortiGate and partial session information for internet traffic from a user on the internal network.

If the priority on route ID _ were changed from 10 to 0, what would happen to traffic matching that user session?

Options:

A- The session would be deleted, and the client would need to start a new session.

B- The session would remain in the session table, but its traffic would now egress from both port1. andport2.

C- The session would remain in the session table, and its traffic would egress from port2.

D- The session would remain in the session table, and its traffic would egress from port1.

Answer:

C

Explanation:

The exhibits show the configuration of static routes and a session table entry for an active session. The static routes are configured with different priorities:

Route through port1 with a gateway of 10.200.1.254 and priority 5.

Route through port2 with a gateway of 10.200.2.254 and priority 10.

If the priority of the route through port2 is changed from 10 to 0, this route will become more preferred than the route through port1 because lower priority values indicate higher preference. As a result, the traffic for the existing session will switch to using the more preferred route:

The session would remain active in the session table, as FortiGate does not immediately clear sessions upon route changes unless explicitly configured to do so.

The traffic for the session would then start egressing from port2, which now has the higher priority route due to its lower priority value.

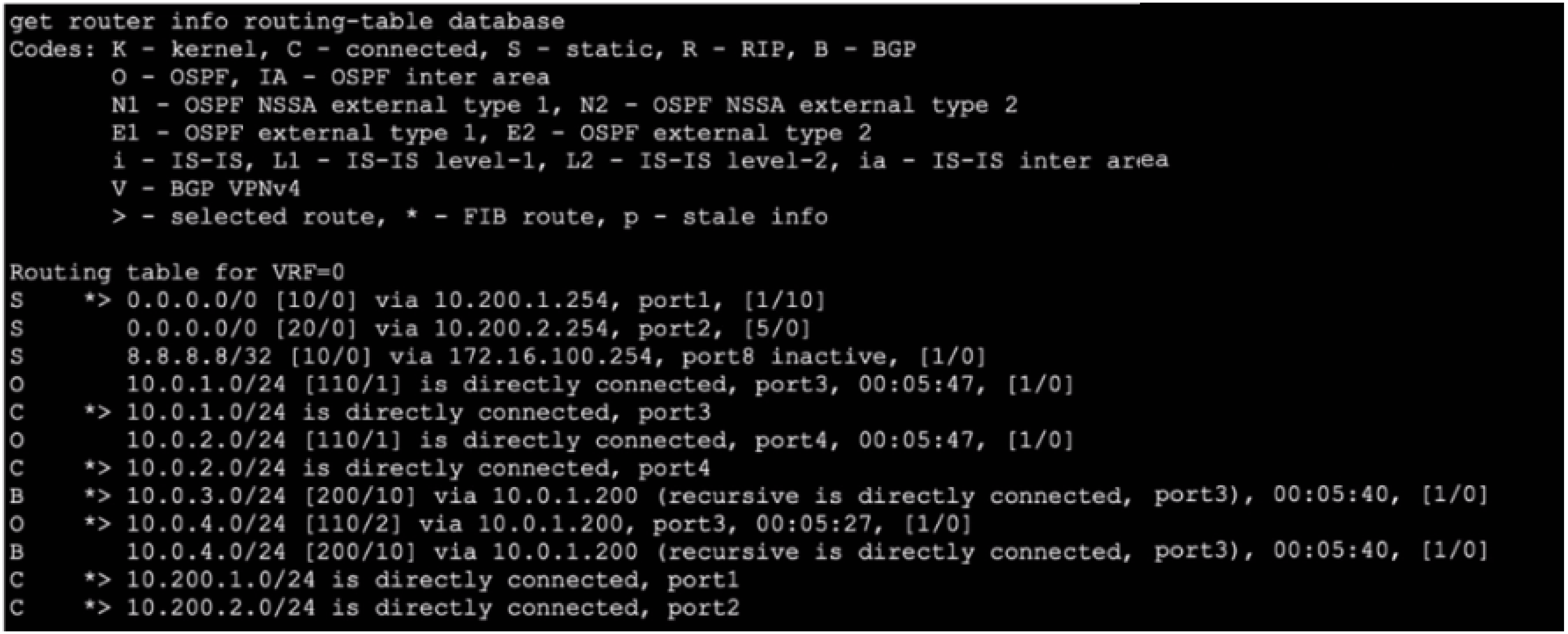
Fortinet Documentation on Routing Configuration

Fortinet Community on Session Handling

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



```
get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S     *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/10]
S        0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S        8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0]
O        10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C     *> 10.0.1.0/24 is directly connected, port3
O        10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C     *> 10.0.2.0/24 is directly connected, port4
B     *> 10.0.3.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
O     *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B        10.0.4.0/24 [200/10] via 10.0.1.200 (recursive is directly connected, port3), 00:05:40, [1/0]
C     *> 10.200.1.0/24 is directly connected, port1
C     *> 10.200.2.0/24 is directly connected, port2
```

Refer to the exhibit, which shows the modified output of the routing kernel.

Which statement is true?

Options:

A- The BGP route to 10.0.4.0/24 is not in the forwarding information base.

B- The default static route through port2 is in the forwarding information base.

C- The default static route through 10.200.1.254 is not in the forwarding information base.

D- The egress interface associated with static route 8.8.8.8/32 is administratively up.

Answer:

B

Explanation:

The routing table shown in the exhibit lists all the routes known to the FortiGate device. It includes routes learned through different protocols such as BGP, OSPF, and static routes.

The entry S * 0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0] indicates that there is a static route to the default gateway (0.0.0.0/0) through port2 with a gateway IP of 10.200.2.254.

The asterisk * next to the route signifies that this route is selected and currently active in the forwarding information base (FIB). This means the FortiGate uses this route to forward packets destined for addresses not otherwise specified in the routing table.

Fortinet Documentation on Routing Table

Fortinet Community Discussion on Routing

20%
DISCOUNT