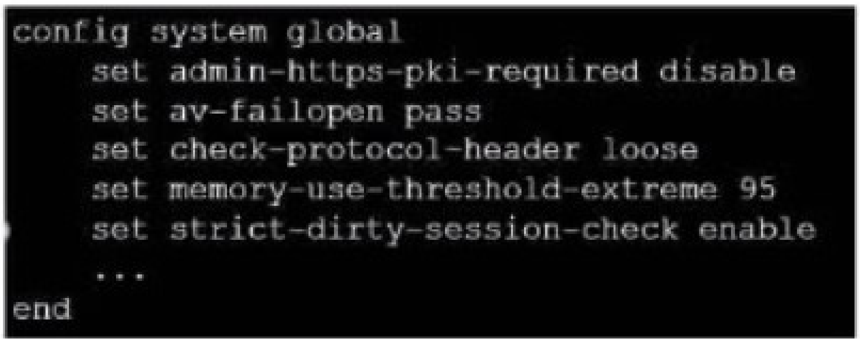
NSE7_EFW-7.2$^{\text{Q\&As}}$

Fortinet NSE 7 - Enterprise Firewall 7.2

QUESTION 1

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

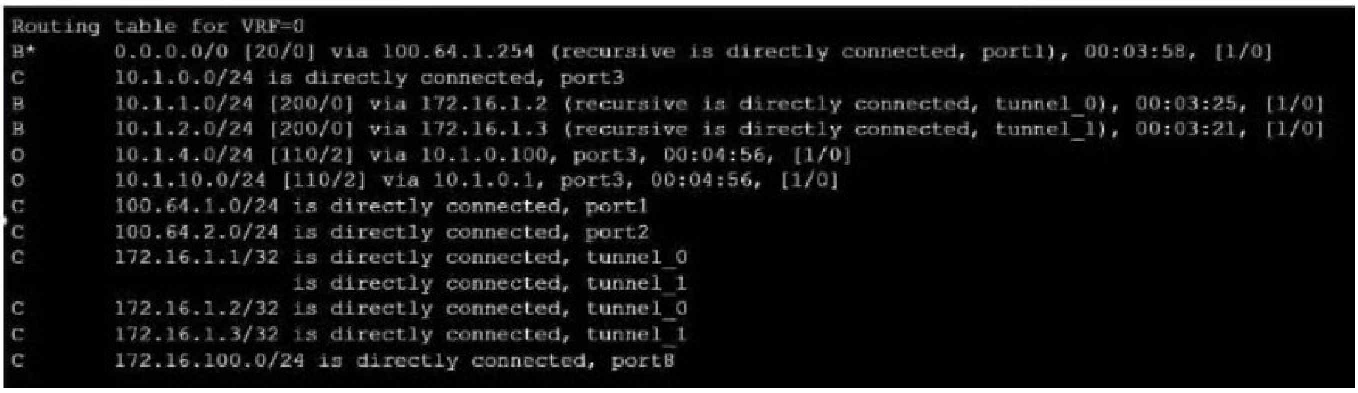
D. NPs and CPs arc disabled

Correct Answer: D

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

QUESTION 2

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: BD

Option B is correct because the routing table shows that the tunnel interfaces have a netmask of 255.255.255.255, which indicates that net-device is enabled in the phase 1 configuration. This option allows the FortiGate to use the tunnel interface as a next-hop for routing, without adding a route to the phase 2 destination1. Option D is correct because the routing table does not show any routes to the phase 2 destination networks, which indicates that add-route is disabled in the phase 1 configuration. This option controls whether the FortiGate adds a static route to the phase 2 destination network using the tunnel interface as the gateway2. Option A is incorrect because IPSec tunnel aggregation is a feature that allows multiple phase 2 selectors to share a single phase 1 tunnel, reducing the number of tunnels and improving performance3. This feature is not related to the routing table or the phase 1 configuration. Option C is incorrect because OSPF is a dynamic routing protocol that can run over IPSec tunnels, but it requires additional configuration on the FortiGate and the peer device4. This option is not related to the routing table or the phase 1 configuration. References: =

1: Technical Tip: `set net-device\\' new route-based IPsec logic2

2: Adding a static route5

3: IPSec VPN concepts6

4: Dynamic routing over IPsec VPN7

QUESTION 3

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

Correct Answer: D

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.

QUESTION 4

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: AC

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. References: =

1: Group address objects synchronized from FortiManager5

2: Security Fabric address object unification6

3: Configuration synchronization7

4: Configuration synchronization7 : Security Fabric - Fortinet Documentation

QUESTION 5

Which two statements about the Security fabric are true? (Choose two.)

A. FortiGate uses the FortiTelemetry protocol to communicate with FortiAnatyzer.

B. Only the root FortiGate sends logs to FortiAnalyzer

C. Only FortiGate devices with configuration-sync receive and synchronize global CMDB objects that the toot FortiGate sends

D. Only the root FortiGate collects network topology information and forwards it to FortiAnalyzer

Correct Answer: BC

In the Security Fabric, only the root FortiGate sends logs to FortiAnalyzer (B). Additionally, only FortiGate devices withconfiguration-syncenabled receive and synchronize global Central Management Database (CMDB) objects that the root FortiGate sends (C). FortiGate uses the FortiTelemetry protocol to communicate with other FortiGates, not FortiAnalyzer (A). The last option (D) is incorrect as all FortiGates can collect and forward network topology information to FortiAnalyzer. References: FortiOS Handbook - Security Fabric