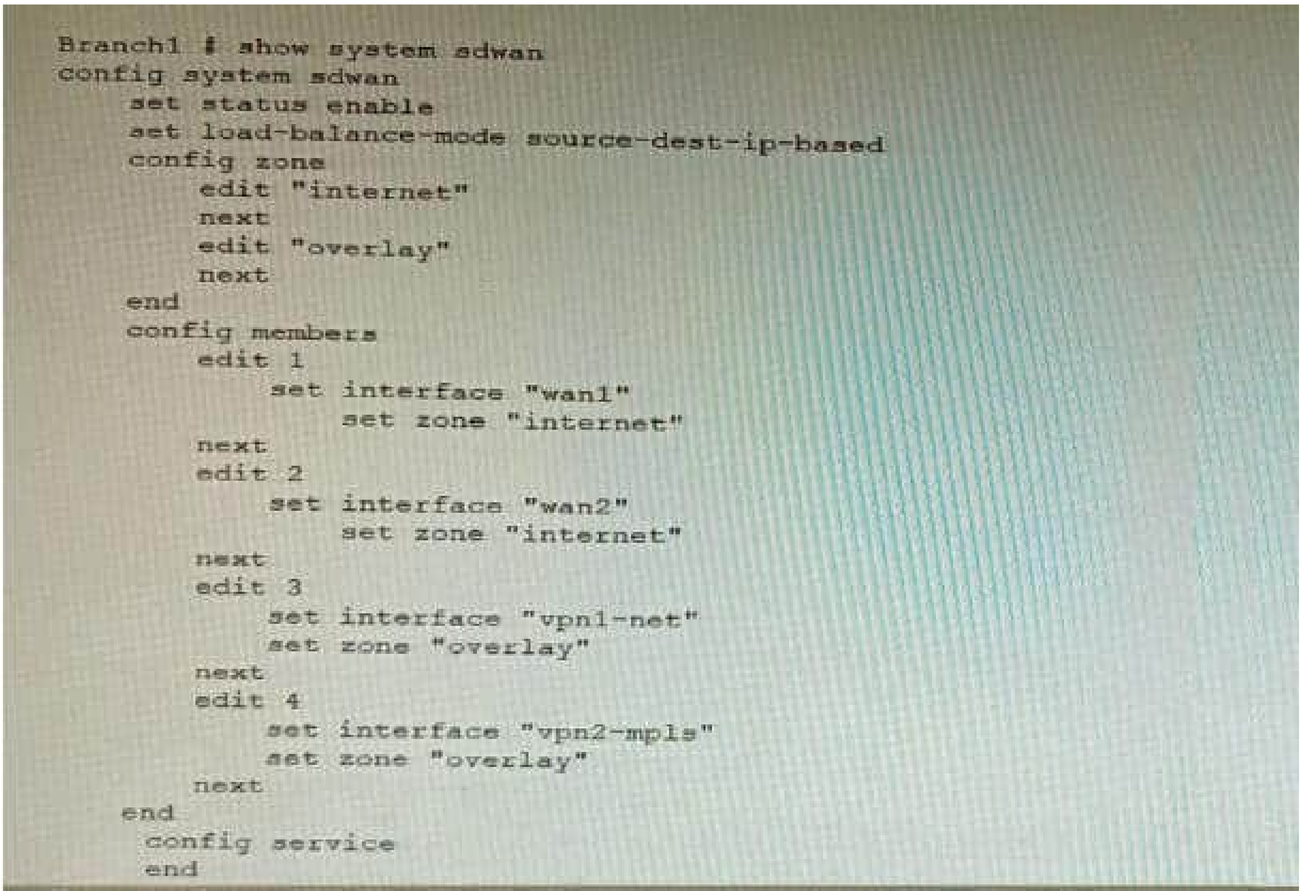
NSE8_812$^{\text{Q\&As}}$

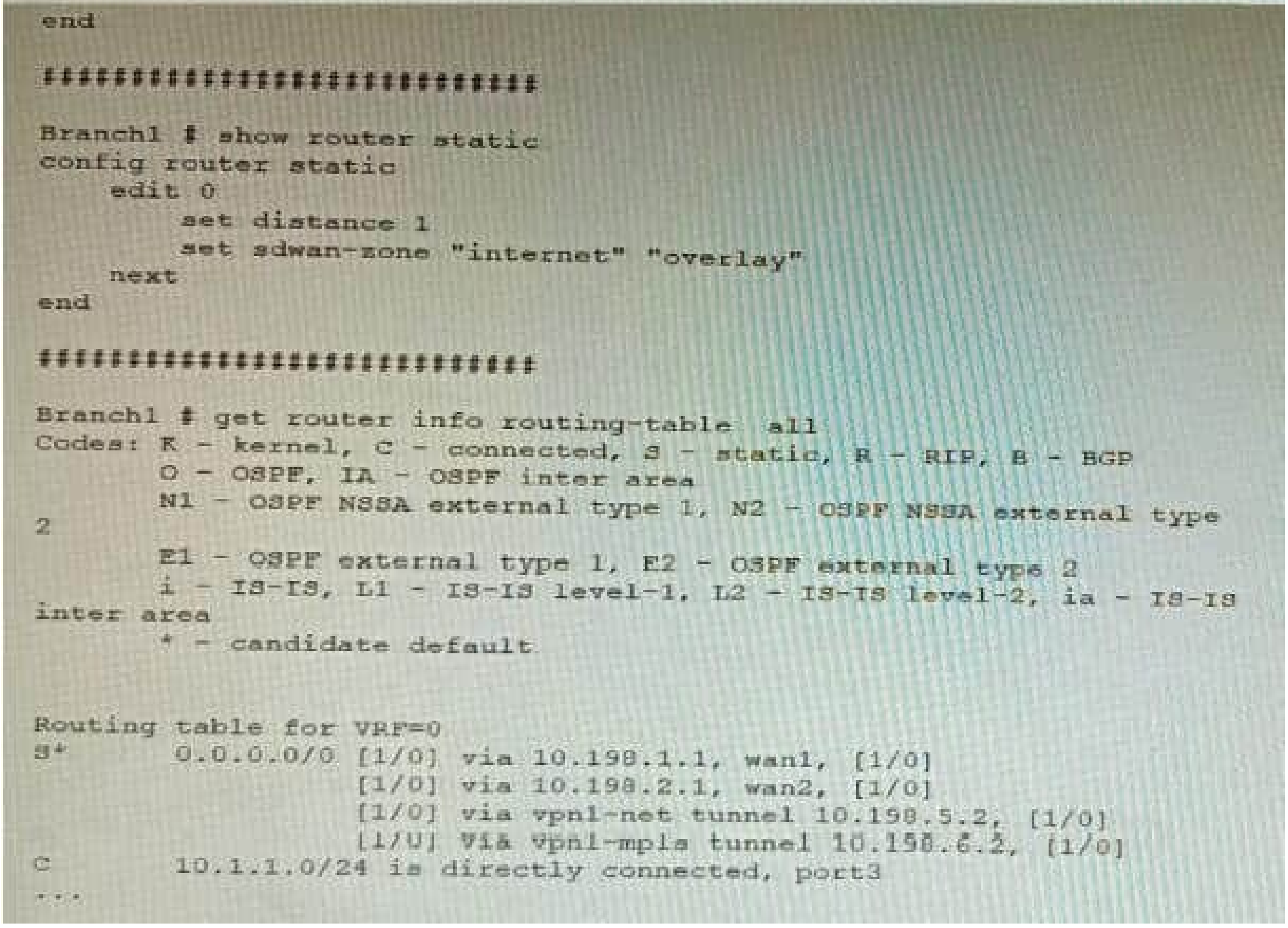
Network Security Expert 8 Written Exam

QUESTION 1

Refer to the exhibit, which shows a Branch1 configuration and routing table. In the SD-WAN implicit rule, you do not want the traffic load balance for the overlay interface when all members are available.



```
Branch1 # show system sdwan
config system sdwan
    set status enable
    set load-balance-mode source-dest-ip-based
    config zone
        edit "internet"
        next
        edit "overlay"
        next
    end
    config members
        edit 1
            set interface "wan1"
                set zone "internet"
        next
        edit 2
            set interface "wan2"
                set zone "internet"
        next
        edit 3
            set interface "vpn1-net"
            set zone "overlay"
        next
        edit 4
            set interface "vpn2-mpls"
            set zone "overlay"
        next
    end
     config service
     end
```



```
end

##############################

Branch1 # show router static
config router static
    edit 0
        set distance 1
        set sdwan-zone "internet" "overlay"
    next
end

##############################

Branch1 # get router info routing-table  all
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
       * - candidate default


Routing table for VRF=0
S*        0.0.0.0/0 [1/0] via 10.198.1.1, wan1, [1/0]
                    [1/0] via 10.198.2.1, wan2, [1/0]
                    [1/0] via vpn1-net tunnel 10.198.5.2, [1/0]
                    [1/U] Via vpn1-mpls tunnel 10.158.6.2, [1/0]
C         10.1.1.0/24 is directly connected, port3
...
```

In this scenario, which configuration change will meet this requirement?

A. Change the load-balance-mode to source-ip-based.

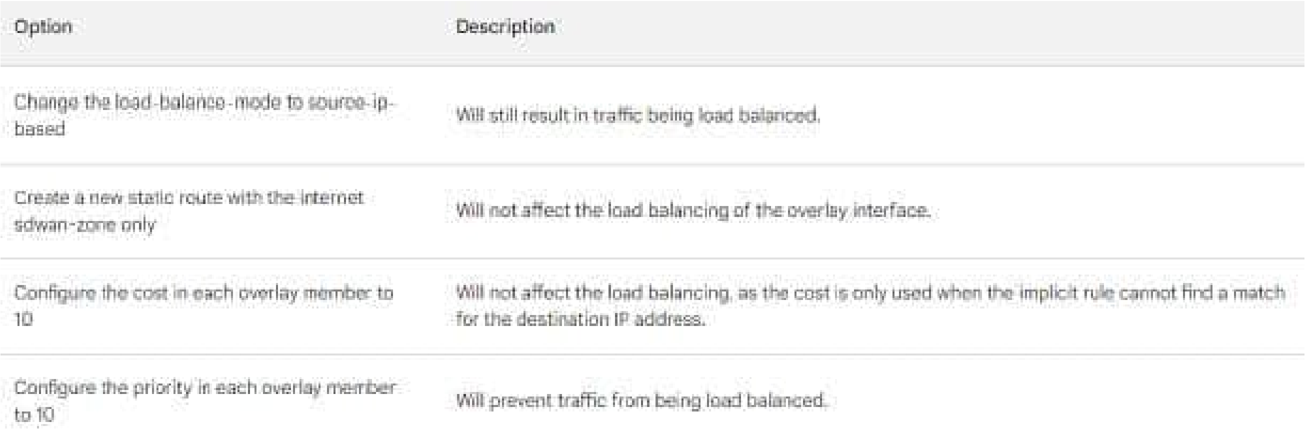
B. Create a new static route with the internet sdwan-zone only

C. Configure the cost in each overlay member to 10.

D. Configure the priority in each overlay member to 10.

Correct Answer: D

Explanation: The default load balancing mode for the SD-WAN implicit rule is source IP based. This means that traffic will be load balanced evenly between the overlay members, regardless of the member\\'s priority. To prevent traffic from being load balanced, you can configure the priority of each overlay member to 10. This will make the member ineligible for load balancing. The other options are not correct. Changing the load balancing mode to source-IP based will still result in traffic being load balanced. Creating a new static route with the internet sdwan-zone only will not affect the load balancing of the overlay interface. Configuring the cost in each overlay member to 10 will also not affect the load balancing, as the cost is only used when the implicit rule cannot find a match for the destination IP address.



Option	Description
Change the load-balance-mode to source-ip-based	Will still result in traffic being load balanced.
Create a new static route with the internet sdwan-zone only	Will not affect the load balancing of the overlay interface.
Configure the cost in each overlay member to 10	Will not affect the load balancing, as the cost is only used when the implicit rule cannot find a match for the destination IP address.
Configure the priority in each overlay member to 10	Will prevent traffic from being load balanced.

QUESTION 2

Refer to the exhibits.

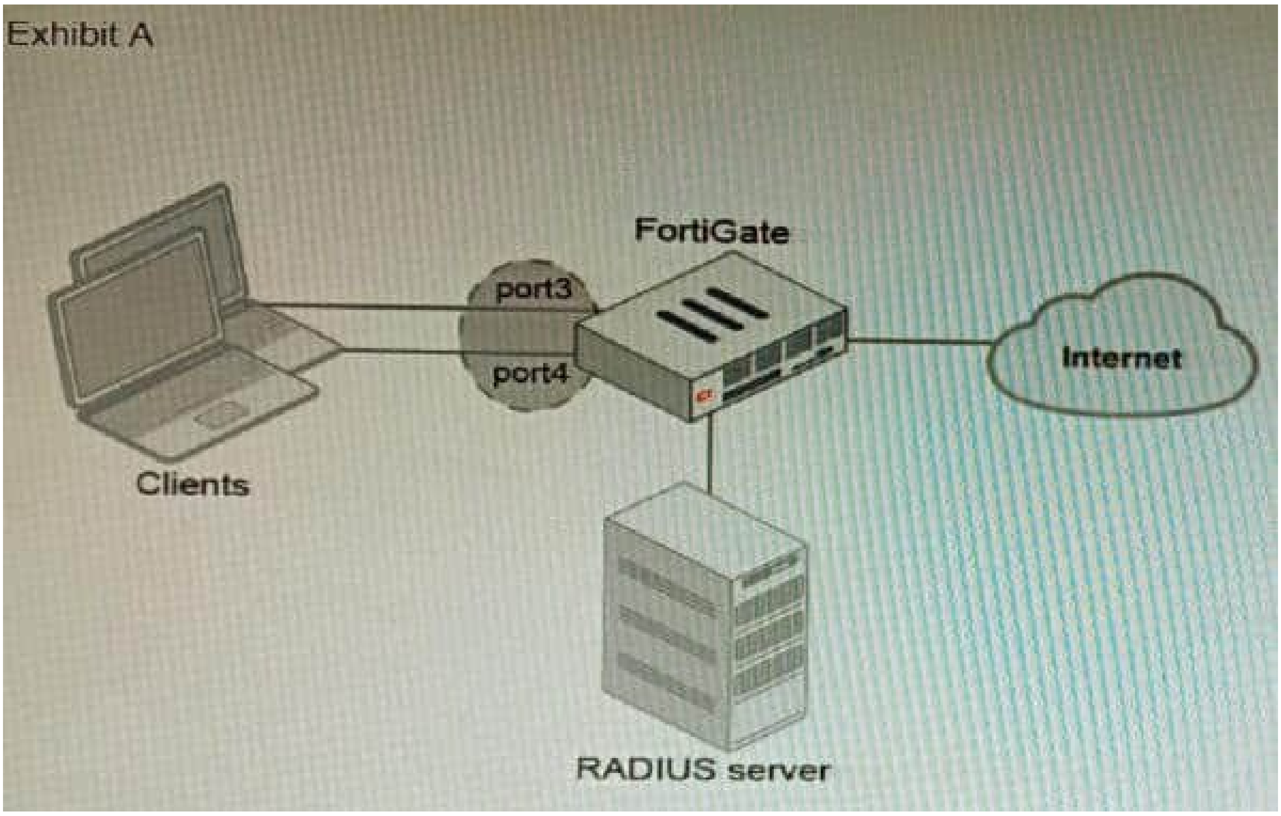


Exhibit A
FortiGate
port3
port4
Internet
Clients
RADIUS server

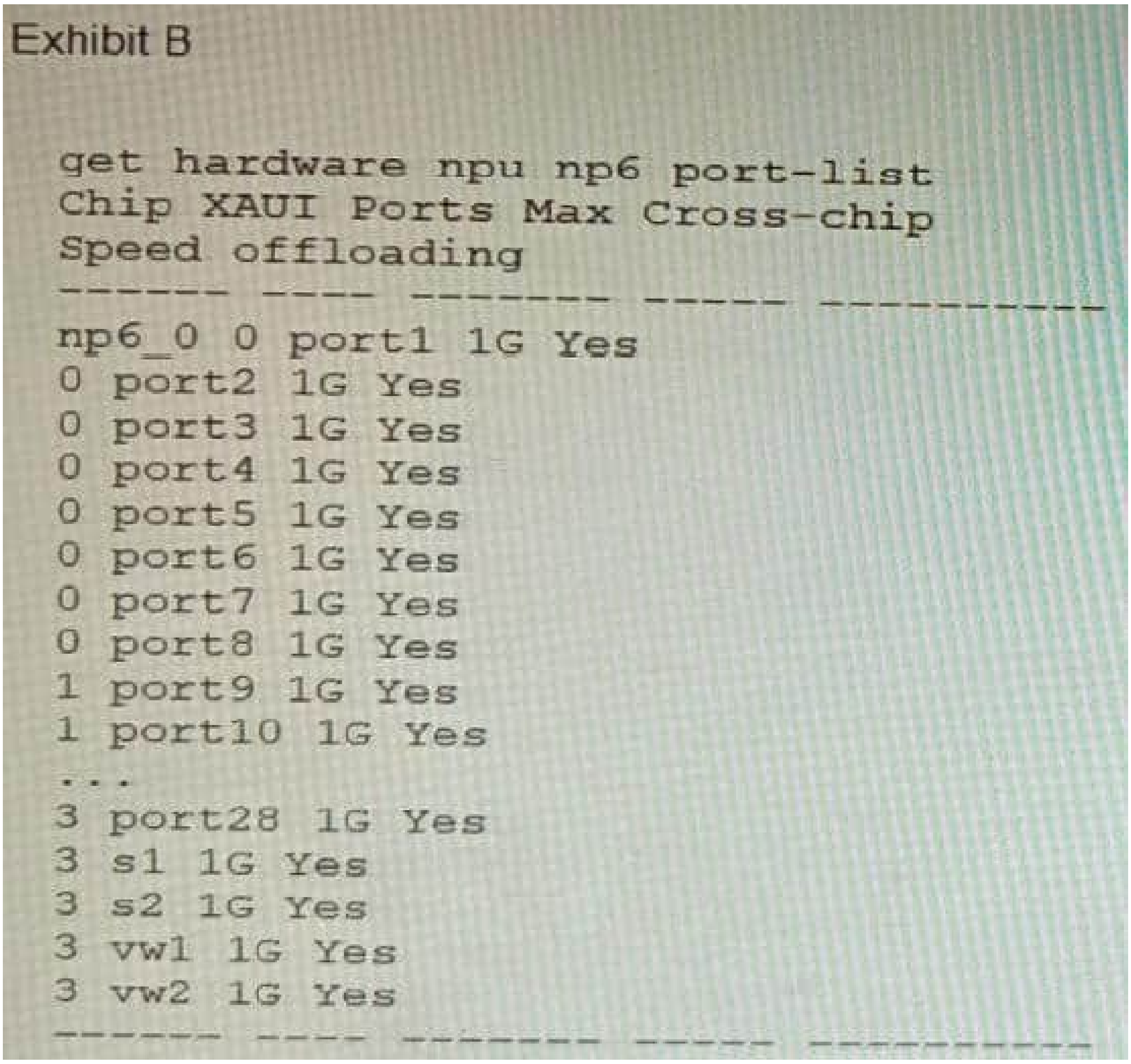


Exhibit B

```
get hardware npu np6 port-list
Chip XAUI Ports Max Cross-chip
Speed offloading
------ ---- ------- ----- ----------
np6_0 0 port1 1G Yes
0 port2 1G Yes
0 port3 1G Yes
0 port4 1G Yes
0 port5 1G Yes
0 port6 1G Yes
0 port7 1G Yes
0 port8 1G Yes
1 port9 1G Yes
1 port10 1G Yes
...
3 port28 1G Yes
3 s1 1G Yes
3 s2 1G Yes
3 vw1 1G Yes
3 vw2 1G Yes
------ ---- ------- ----- ----------
```

A customer is looking for a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E.

Referring to the exhibits, which two conditions allow authentication to the client devices before assigning an IP address? (Choose two.)

A. FortiGate devices with NP6 and hardware switch interfaces cannot support 802.1X authentication.

B. Devices connected directly to ports 3 and 4 can perform 802 1X authentication.

C. Ports 3 and 4 can be part of different switch interfaces.

D. Client devices must have 802 1X authentication enabled

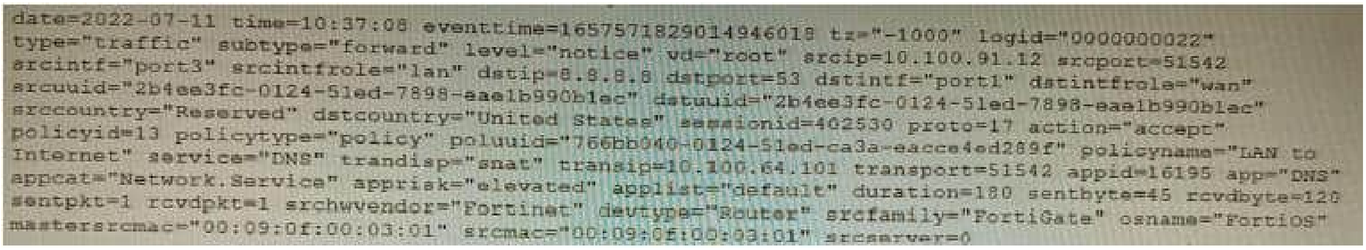
Correct Answer: BD

Explanation: The customer wants to deploy a solution to authenticate the clients connected to a hardware switch interface of a FortiGate 400E device. A hardware switch interface is an interface that combines multiple physical interfaces into one logical interface, allowing them to act as a singleswitch with one IP address and one set of security policies. The customer wants to use 802.1X authentication for this solution, which is a standard protocol for port-based network access control (PNAC) that authenticates clients based on their credentials before granting them access to

network resources. One condition that allows authentication to the client devices before assigning an IP address is that devices connected directly to ports 3 and 4 can perform 802.1X authentication. This is because ports 3 and 4 are part of the hardware switch interface named "lan", which has an IP address of 10.10.10.254/24 and an inbound SSL inspection profile named "sslinspection". The inbound SSL inspection profile enables the FortiGate device to intercept and inspect SSL/TLS traffic from clients before forwarding it to servers, which allows it to apply security policies and features such as antivirus, web filtering, application control, etc. However, before performing SSL inspection, the FortiGate device needs to authenticate the clients using 802.1X authentication, which requires the clients to send their credentials (such as username and password) to the FortiGate device over a secure EAP (Extensible Authentication Protocol) channel. The FortiGate device then verifies the credentials with an authentication server (such as RADIUS or LDAP) and grants or denies access to the clients based on the authentication result. Therefore, devices connected directly to ports 3 and 4 can perform 802.1X authentication before assigning an IP address. Another condition that allows authentication to the client devices before assigning an IP address is that client devices must have 802.1X authentication enabled. This is because 802.1X authentication is a mutual process that requires both the client devices and the FortiGate device to support and enable it. The client devices must have 802.1X authentication enabled in their network settings, which allows them to initiate the authentication process when they connect to the hardware switch interface of the FortiGate device. The client devices must also have an 802.1X supplicant software installed, which is a program that runs on the client devices and handles the communication with the FortiGate device using EAP messages. The client devices must also have a trusted certificate installed, which is used to verify the identity of the FortiGate device and establish a secure EAP channel. Therefore, client devices must have 802.1X authentication enabled before assigning an IP address.
References: https:// docs.fortinet.com/document/fortigate/7.0.0/administration- guide/19662/hardware-switchinterfaceshttps://docs.fortinet.com/document/fortigate/7.0.0/administration- guide/19662/802-1x-authentication

QUESTION 3

You must analyze an event that happened at 20:37 UTC. One log relevant to the event is extracted from FortiGate logs:



```
date=2022-07-11 time=10:37:08 eventtime=1657571829014946018 tz="-1000" logid="0000000022"
type="traffic" subtype="forward" level="notice" vd="root" srcip=10.100.91.12 srcport=51542
srcintf="port3" srcintfrole="lan" dstip=8.8.8.8 dstport=53 dstintf="port1" dstintfrole="wan"
srcuuid="2b4ee3fc-0124-51ed-7898-eae1b990b1ec" dstuuid="2b4ee3fc-0124-51ed-7898-eae1b990b1ec"
srccountry="Reserved" dstcountry="United States" sessionid=402530 proto=17 action="accept"
policyid=13 policytype="policy" poluuid="766bb040-0124-51ed-ca3a-eacce4ed289f" policyname="LAN to
Internet" service="DNS" trandisp="snat" transip=10.100.64.101 transport=51542 appid=16195 app="DNS"
appcat="Network.Service" apprisk="elevated" applist="default" duration=180 sentbyte=45 rcvdbyte=120
sentpkt=1 rcvdpkt=1 srchwvendor="Fortinet" devtype="Router" srcfamily="FortiGate" osname="FortiOS"
mastersrcmac="00:09:0f:00:03:01" srcmac="00:09:0f:00:03:01" srcserver=0
```

The devices and the administrator are all located in different time zones Daylight savings time (DST) is disabled The FortiGate is at GMT-1000. The FortiAnalyzer is at GMT-0800 Your browser local time zone is at GMT-03.00

You want to review this log on FortiAnalyzer GUI, what time should you use as a filter?

A. 20:37:08

B. 10:37:08

C. 17:37:08

D. 12.37:08

Correct Answer: C

Explanation: To review this log on FortiAnalyzer GUI, the administrator should use the time filter that matches the local time zone of FortiAnalyzer, which is GMT-0800. Since the log was generated at 20:37 UTC (GMT+0000), the corresponding time in GMT-0800 is

20:37 - 8 hours = 12:37. However, since DST is disabled on FortiAnalyzer, the administrator should add one hour to account for daylight saving time difference, resulting in 12:37 + 1 hour = 13:37. Therefore, the time filter to use is 13:37:08. References:https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration- guide/103664/time-zone-and-daylight-saving-time

QUESTION 4

A customer with a FortiDDoS 200F protecting their fibre optic internet connection from incoming traffic sees that all the traffic was dropped by the device even though they were not under a DoS attack. The traffic flow was restored after it was rebooted using the GUI. Which two options will prevent this situation in the future? (Choose two)

A. Change the Adaptive Mode.

B. Create an HA setup with a second FortiDDoS 200F

C. Move the internet connection from the SFP interfaces to the LC interfaces

D. Replace with a FortiDDoS 1500F

Correct Answer: BD

B is correct because creating an HA setup with a second FortiDDoS 200F will provide redundancy in case one of the devices fails. This will prevent all traffic from being dropped in the event of a failure.

D is correct because the FortiDDoS 1500F has a larger throughput capacity than the FortiDDoS 200F. This means that it will be less likely to drop traffic even under heavy load.

The other options are incorrect. Option A is incorrect because changing the Adaptive Mode will not prevent the device from dropping traffic. Option C is incorrect because moving the internet connection from the SFP interfaces to the LC

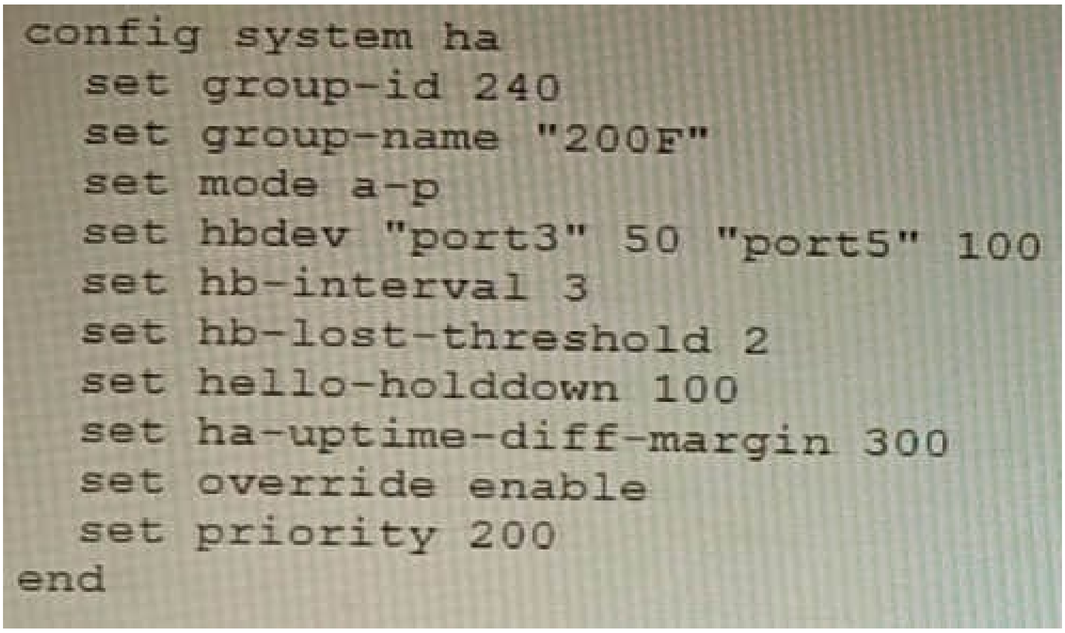
interfaces will not change the throughput capacity of the device.

References:

FortiDDoS 200F Datasheet | Fortinet Document Library FortiDDoS 1500F Datasheet | Fortinet Document Library High Availability (HA) on FortiDDoS | FortiDDoS / FortiOS 7.0.0 - Fortinet Document Library

QUESTION 5

An HA topology is using the following configuration:



```
config system ha
   set group-id 240
   set group-name "200F"
   set mode a-p
   set hbdev "port3" 50 "port5" 100
   set hb-interval 3
   set hb-lost-threshold 2
   set hello-holddown 100
   set ha-uptime-diff-margin 300
   set override enable
   set priority 200
end
```

Based on this configuration, how long will it take for a failover to be detected by the secondary cluster member?

A. 600ms

B. 200ms

C. 300ms

D. 100ms

Correct Answer: B

Explanation: The HA heartbeat interval is 100ms, and the number of lost heartbeats before a failover is detected is 2. So, it will take 2 * 100ms = 200ms for a failover to be detected by the secondary cluster member.

Reference:

FortiGate High Availability:

https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/647723/link- monitoring-and-ha-failover-time