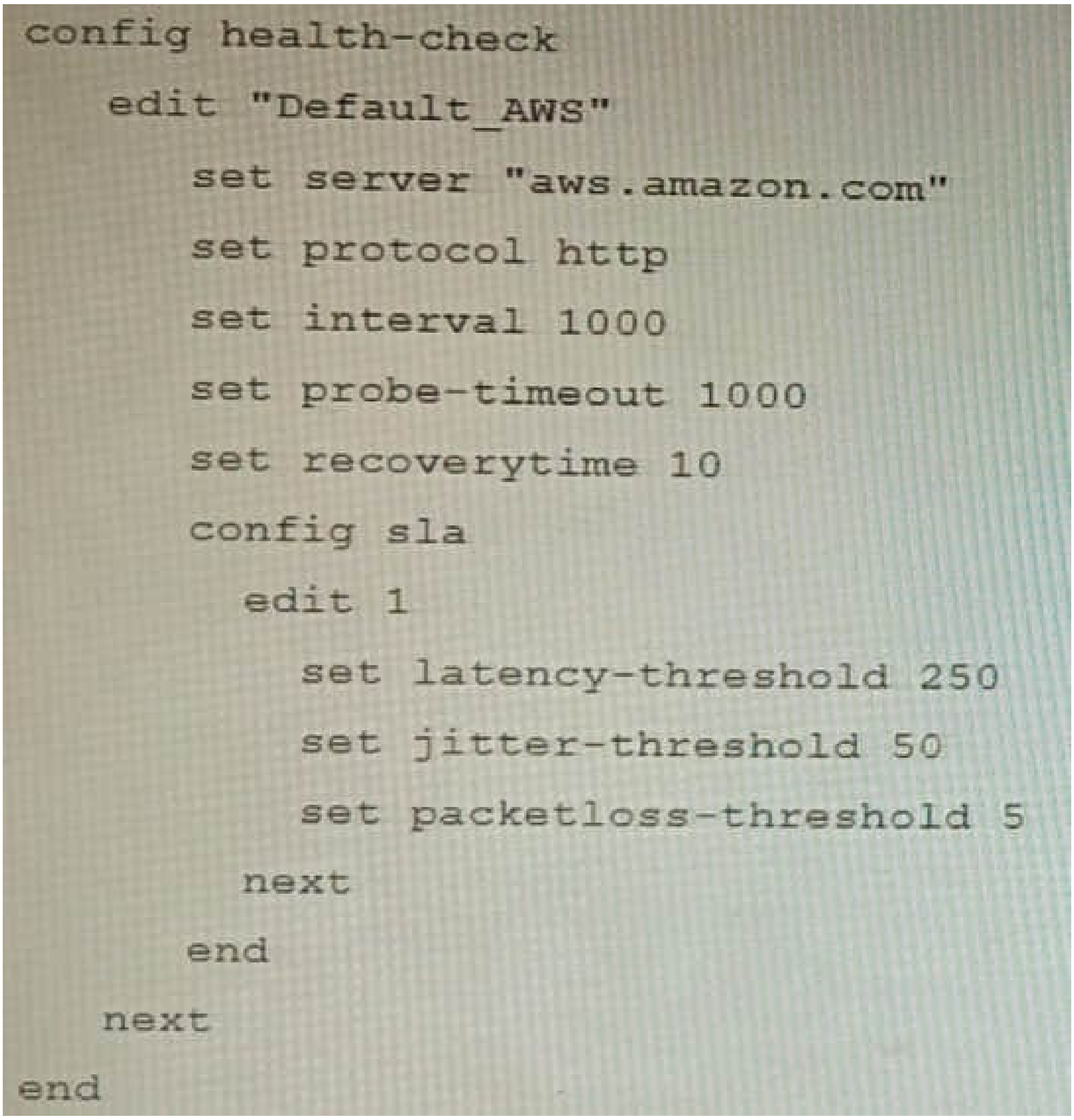
NSE8_812$^{Q\&As}$

Network Security Expert 8 Written Exam

QUESTION 1

You are creating the CLI script to be used on a new SD-WAN deployment You will have branches with a different number of internet connections and want to be sure there is no need to change the Performance SLA configuration in case more connections are added to the branch.

The current configuration is:



```
config health-check
    edit "Default_AWS"
        set server "aws.amazon.com"
        set protocol http
        set interval 1000
        set probe-timeout 1000
        set recoverytime 10
        config sla
            edit 1
                set latency-threshold 250
                set jitter-threshold 50
                set packetloss-threshold 5
            next
        end
    next
end
```

Which configuration do you use for the Performance SLA members?

A. set members any

B. set members 0

C. current configuration already fulfills the requirement

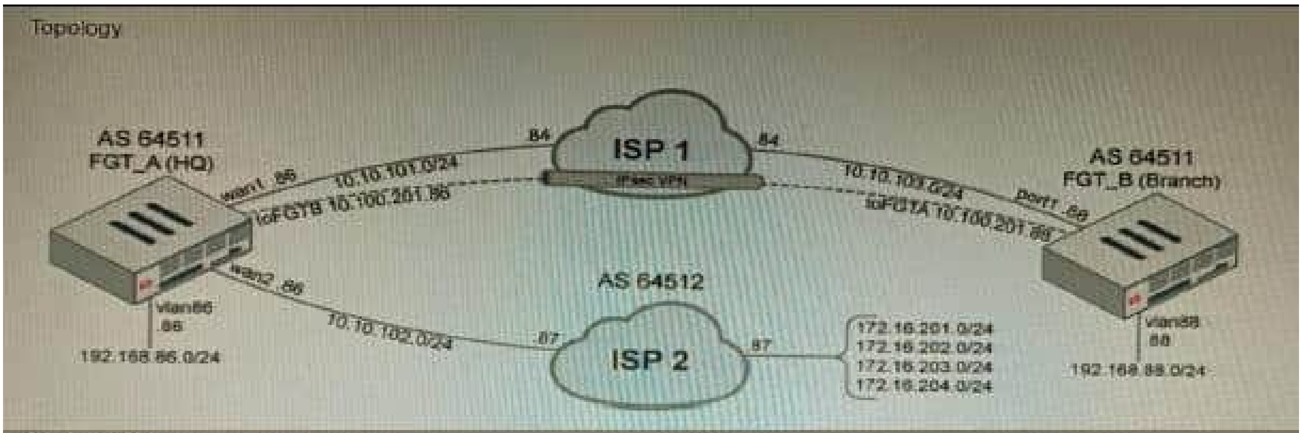
D. set members all

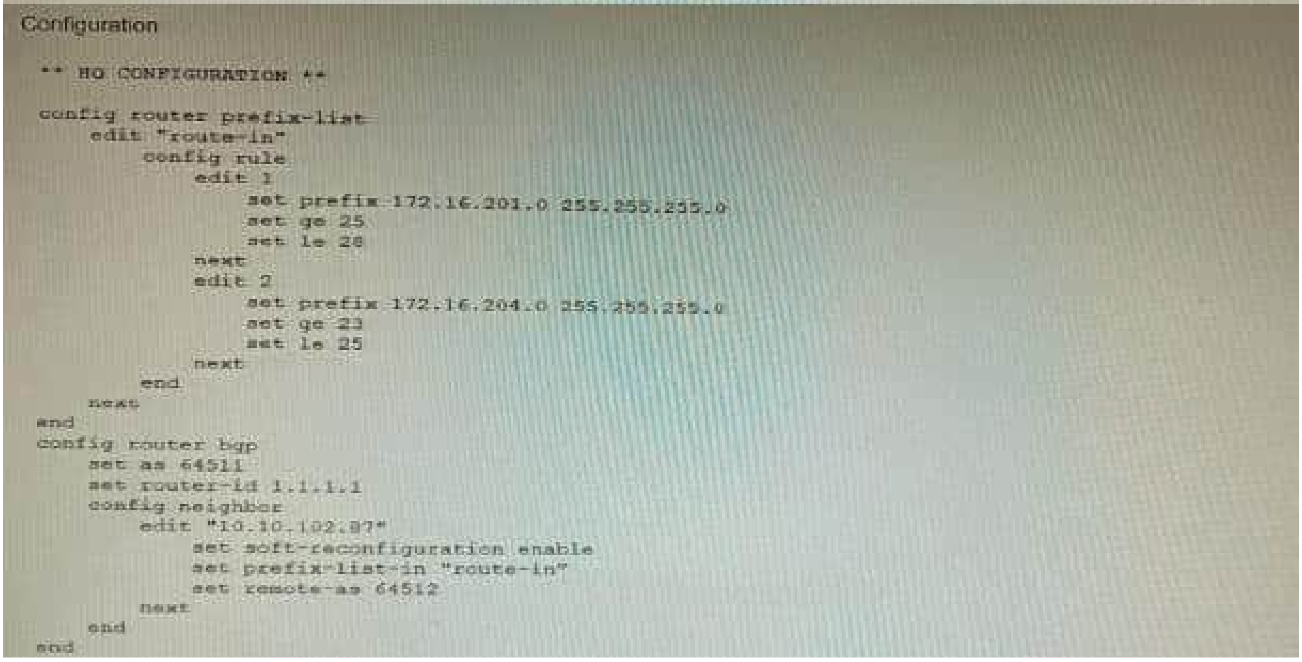
Correct Answer: A

Explanation: The set members any option will ensure that all of the SD-WAN interfaces are included in the Performance SLA. This is the best option if you want to be sure that the Performance SLA will be triggered even if more connections are added to the branch in the future. The set members 0 option will exclude all of the SD-WAN interfaces from the Performance SLA. This is not a good option because it will prevent the Performance SLA from being triggered even if there is a problem with the network. The current configuration already fulfills the requirement option is incorrect because it does not ensure that all of the SD-WAN interfaces will be included in the Performance SLA. The set members all option will include all of the SD-WAN interfaces in the Performance SLA, but it is not the best option because it is not scalable. If you have a large number of SD-WAN interfaces, this option will cause the Performance SLA to be triggered too often. References: Performance SLA | FortiGate / FortiOS 7.4.0 Configuring Performance SLA | FortiGate / FortiOS 7.4.0

QUESTION 2

Refer to the exhibits.




Configuration

```
** HQ CONFIGURATION **

config router prefix-list
    edit "route-in"
        config rule
            edit 1
                set prefix 172.16.201.0 255.255.255.0
                set ge 25
                set le 28
            next
            edit 2
                set prefix 172.16.204.0 255.255.255.0
                set ge 23
                set le 25
            next
        end
    next
end
config router bgp
    set as 64511
    set router-id 1.1.1.1
    config neighbor
        edit "10.10.102.87"
            set soft-reconfiguration enable
            set prefix-list-in "route-in"
            set remote-as 64512
        next
    end
end
```

A customer has deployed a FortiGate with iBGP and eBGP routing enabled. HQ is receiving routes over eBGP from ISP

2; however, only certain routes are showing up in the routing table-Assume that BGP is working perfectly and that the only possible modifications to the routing table are solely due to the prefix list that is applied on HQ.

Given the exhibits, which two routes will be active in the routing table on the HQ firewall? (Choose two.)

A. 172.16.204.128/25

B. 172.16.201.96/29

C. 172,620,64,27

D. 172.16.204.64/27

Correct Answer: AD

Explanation: The prefix list in the exhibit is configured to match prefixes that are either in the 172.16.204.0/24 subnet or in the 172.62.0.0/16 subnet. The routes that match these prefixes will be active in the routing table on the HQ firewall. The

routes that match the following prefixes will not be active in the routing table:

172.16.201.96/29

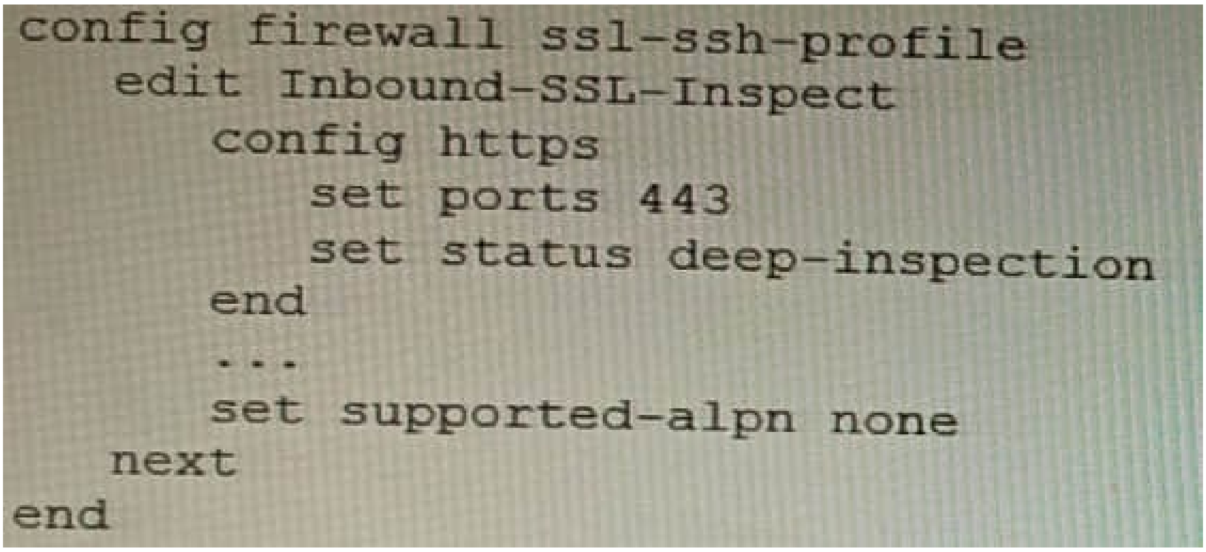
These routes do not match the criteria set by the prefix list.

References:

Prefix lists | FortiGate / FortiOS 7.4.0 - Fortinet Document Library Configuring BGP | FortiGate / FortiOS 7.4.0 - Fortinet Document Library

QUESTION 3

Refer to the CLI configuration of an SSL inspection profile from a FortiGate device configured to protect a web server:



```
config firewall ssl-ssh-profile
    edit Inbound-SSL-Inspect
        config https
            set ports 443
            set status deep-inspection
        end
        ...
        set supported-alpn none
    next
end
```

Based on the information shown, what is the expected behavior when an HTTP/2 request comes in?

A. FortiGate will reject all HTTP/2 ALPN headers.

B. FortiGate will strip the ALPN header and forward the traffic.

C. FortiGate will rewrite the ALPN header to request HTTP/1.

D. FortiGate will forward the traffic without modifying the ALPN header.

Correct Answer: A

Explanation: Thesupported-alpnparameter is set tohttp1.1in the SSL inspection profile. This means that the FortiGate will only accept HTTP/1.1 traffic. Any HTTP/2 traffic will be rejected.

The following is the relevant documentation from Fortinet:

Thesupported-alpnparameter specifies the list of ALPN protocols that the FortiGate will accept. If the client requests a protocol that is not in this list, the FortiGate will reject the connection.

The default value for thesupported-alpnparameter isall. This means that the FortiGate will accept any ALPN protocol that the client requests. To reject all HTTP/2 traffic, set thesupported-alpnparameter tohttp1.1. Source: https://

docs.fortinet.com/document/fortigate/7.0.0/new-features/710924/http-2- support-in-proxy-mode-ssl-inspection

QUESTION 4

A customer\\'s cybersecurity department needs to implement security for the traffic between two VPCs in AWS, but these belong to different departments within the company. The company uses a single region for all their VPCs.

Which two actions will achieve this requirement while keeping separate management of each department\\'s VPC? (Choose two.)

A. Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster.

B. Create an 1AM account for the cybersecurity department to manage both existing VPC, create a FortiGate HA Cluster on each VPC and IPSEC VPN to force traffic between the VPCs through the FortiGate clusters

C. Migrate all the instances to the same VPC and create 1AM accounts for each department, then implement a new subnet for a FortiGate auto-scaling group and use routing tables to force the traffic through the FortiGate cluster.

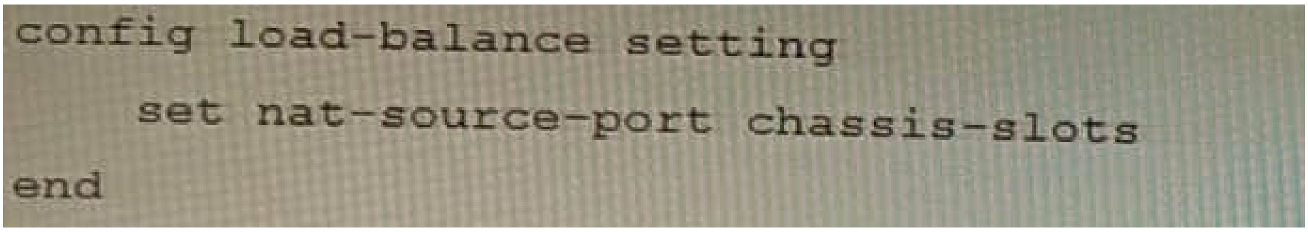
D. Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPC to force routing through the FortiGate cluster

Correct Answer: AD

Explanation: To implement security for the traffic between two VPCs in AWS, while keeping separate management of each department\\'s VPC, two possible actions are: Create a transit VPC with a FortiGate HA cluster, connect to the other two using VPC peering, and use routing tables to force traffic through the FortiGate cluster. This option allows the cybersecurity department to manage the transit VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The VPC peering connections enable direct communication between the VPCs without using public IPs or gateways. The routing tables can be configured to direct all inter-VPC traffic to the transit VPC. Create a VPC with a FortiGate auto-scaling group with a Transit Gateway attached to the three VPCs to force routing through the FortiGate cluster. This option also allows the cybersecurity department to manage the security VPC and apply security policies on the FortiGate cluster, while the other departments can manage their own VPCs and instances. The Transit Gateway acts as a network hub that connects multiple VPCs and on-premises networks. The routing tables can be configured to direct all inter-VPC traffic to the security VPC. References: https://docs.fortinet.com/document/fortigate-public-cloud/7.2.0/aws-administration- guide/506140/connecting-a-localfortigate-to-an-aws-vpc-vpn https://docs.fortinet.com/document/fortigate-public-cloud/7.0.0/sd-wan- architecture-forenterprise/166334/sd-wan-configuration

QUESTION 5

Review the following FortiGate-6000 configuration excerpt:



```
config load-balance setting
    set nat-source-port chassis-slots
end
```

Based on the configuration, which statement is correct regarding SNAT source port partitioning behavior?

A. It dynamically distributes SNAT source ports to operating FPCs or FPMs.

B. It is the default SNAT configuration and preserves active sessions when an FPC or FPM goes down.

C. It statically distributes SNAT source ports to operating FPCs or FPMs

D. It equally distributes SNAT source ports across chassis slots.

Correct Answer: A

Explanation: The configuration excerpt shows that the SNAT source port partitioning behavior is set to dynamic. This means that the FortiGate will dynamically distribute SNAT source ports to operating FPCs or FPMs. This ensures that active

sessions are not interrupted if an FPC or FPM goes down.

The other options are incorrect. Option B is incorrect because the default SNAT configuration is static. Option C is incorrect because the configuration excerpt does not specify that SNAT source ports are statically distributed. Option D is

incorrect because the SNAT source ports are not evenly distributed across chassis slots. Here are some additional details about SNAT source port partitioning behavior:

SNAT source port partitioning behavior can be set to dynamic or static.

The default SNAT configuration is static.

Dynamic SNAT source port partitioning ensures that active sessions are not interrupted if an FPC or FPM goes down.

Static SNAT source port partitioning can improve performance by reducing the number of SNAT lookups.