Free Questions for NSE7_EFW-7.2 by braindumpscollection

Shared by Hahn on 22-07-2024

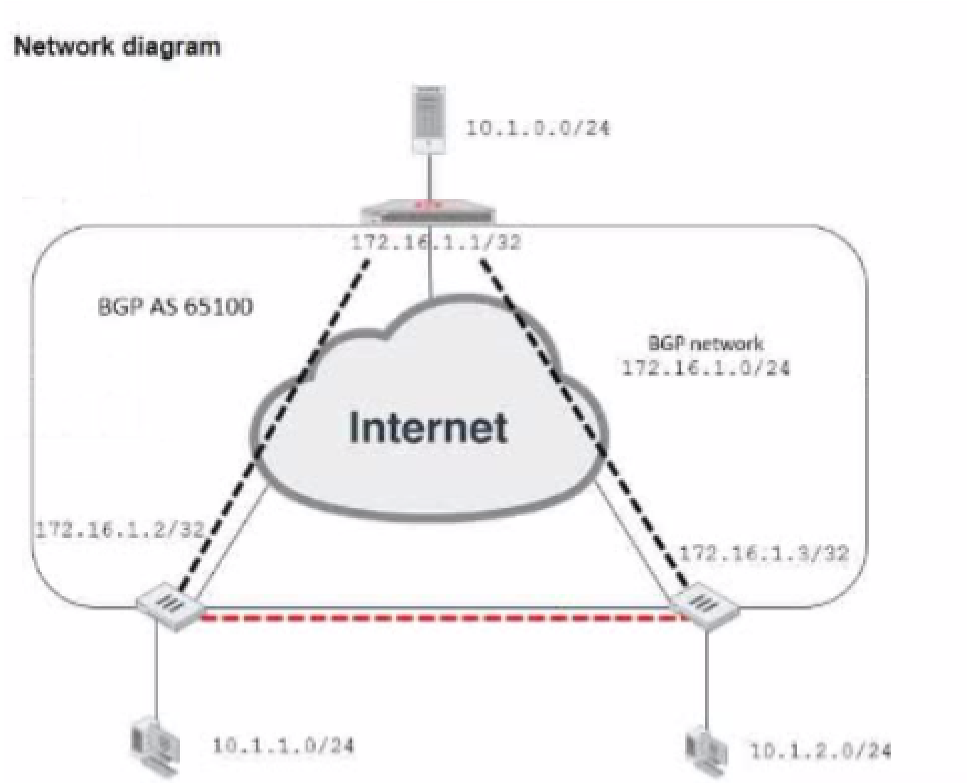
For More Free Questions and Preparation Resources

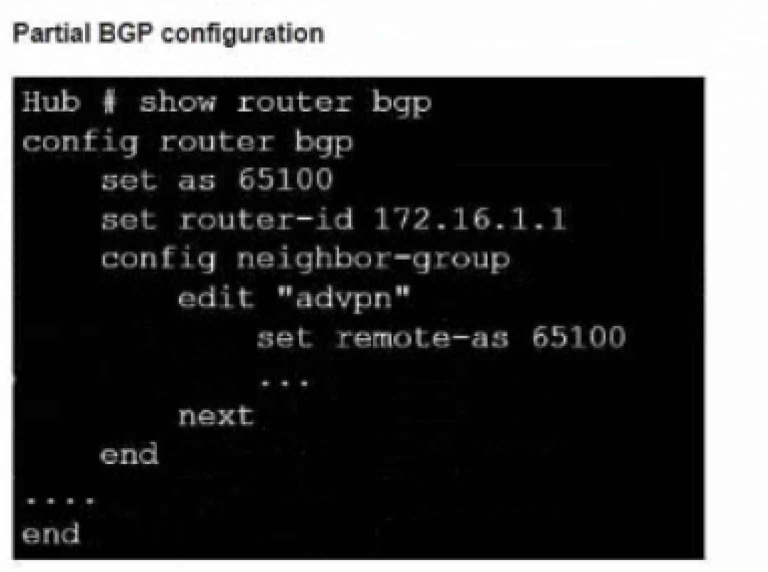
Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Exhibit.





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.)

Options:

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

Answer:

A, C

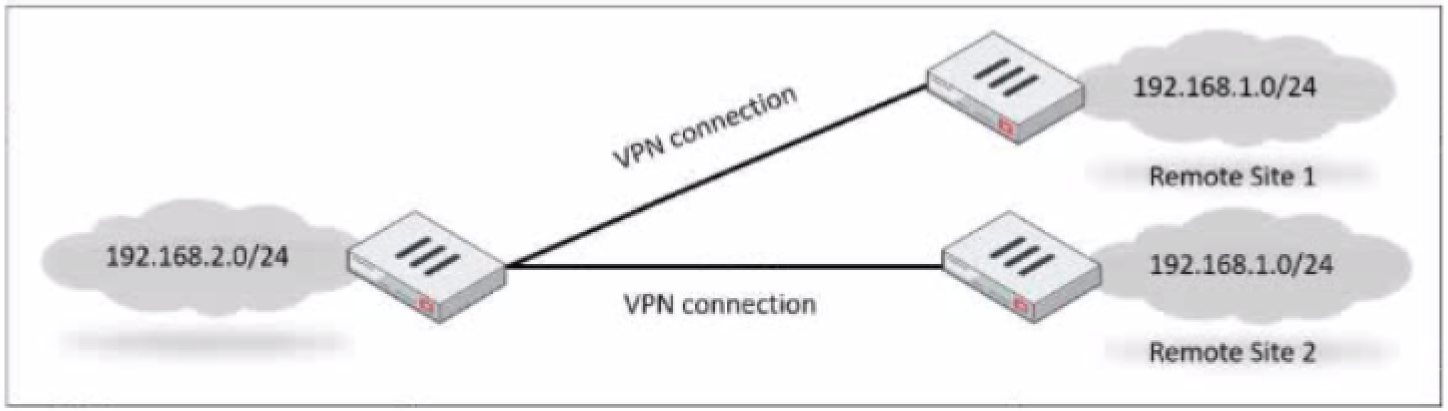
Explanation:

In the ADVPN configuration for BGP, you should specify the prefix that the neighbors can advertise. Option A is correct as you would configure the BGP network prefix that should be advertised to the neighbors, which matches the BGP network in the diagram. Option C is also correct since you should reference the neighbor group configured for the ADVPN setup within the BGP configuration.

Question 2

Question Type: MultipleChoice

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?

Options:

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

Answer:

C

Explanation:

To ensure that only one remote site is connected at any given time in an IPsec VPN scenario, you should use route-overlap with the option to either use-new or use-old. This setting dictates which routes are preferred and how overlaps in routes are handled, allowing for one connection to take precedence over the other (C).

FortiOS Handbook - IPsec VPN

Question 3

Question Type: MultipleChoice

Which, three conditions are required for two FortiGate devices to form an OSPF adjacency? (Choose three.)

Options:

A- OSPF interface network types match

B- OSPF router IDs are unique

C- OSPF interface priority settings are unique

D- OSPF link costs match

E- Authentication settings match

Answer:

A, B, E

Explanation:

Option A is correct because the OSPF interface network types determine how the routers form adjacencies and exchange LSAs on a network segment.The network types must match for the routers to become neighbors1.

Option B is correct because the OSPF router IDs are used to identify each router in the OSPF domain and to establish adjacencies.The router IDs must be unique for the routers to become neighbors2.

Option E is correct because the authentication settings control how the routers authenticate each other before exchanging OSPF packets.The authentication settings must match for the routers to become neighbors3.

Option C is incorrect because the OSPF interface priority settings are used to elect the designated router (DR) and the backup designated router (BDR) on a broadcast or non-broadcast multi-access network.The priority settings do not have to be unique for the routers to become neighbors, but they affect the DR/BDR election process4.

Option D is incorrect because the OSPF link costs are used to calculate the shortest path to a destination network based on the bandwidth of the links.The link costs do not have to match for the routers to become neighbors, but they affect the routing decisions5.Reference: =

1: OSPF network types

2: OSPF router ID

3: OSPF authentication

4: OSPF interface priority

5: OSPF link cost

Question 4

Question Type: **MultipleChoice**

After enabling IPS you receive feedback about traffic being dropped.

What could be the reason?

Options:

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

Answer:

D

Explanation:

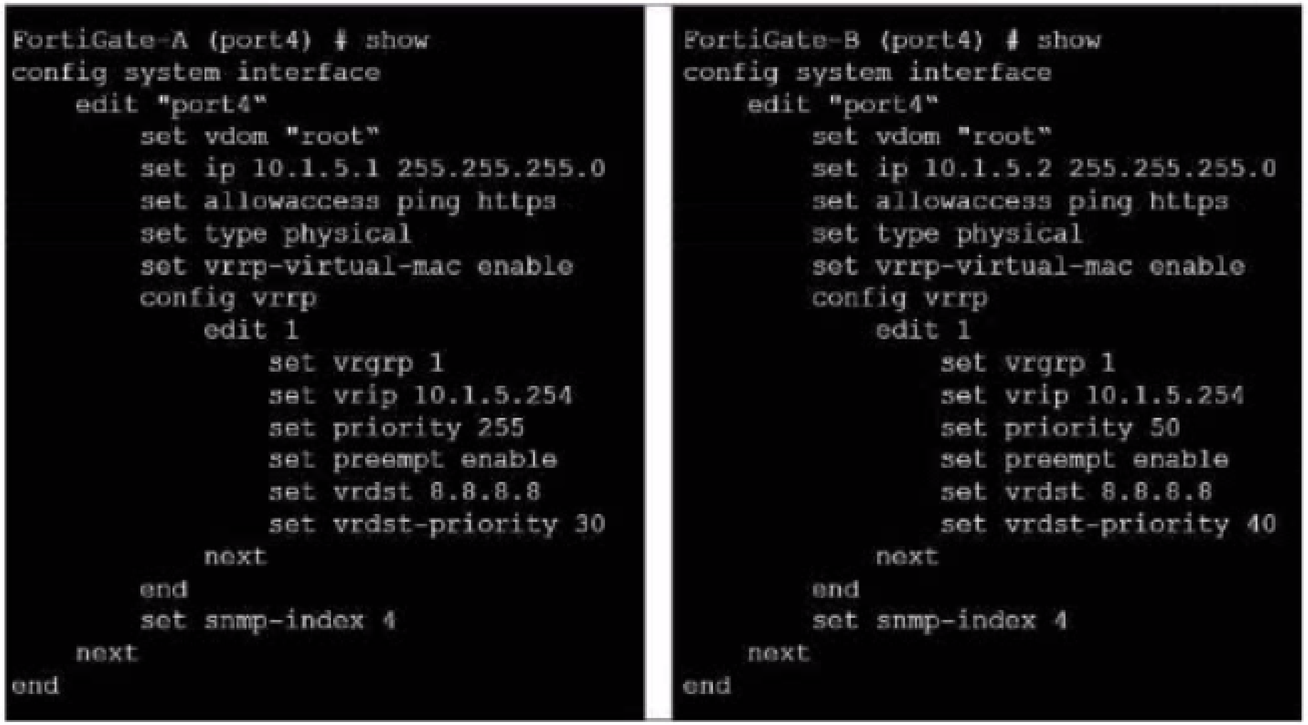
Fail-open is a feature that allows traffic to pass through the IPS sensor without inspection when the sensor fails or is overloaded.If fail-open is set to disable, traffic will be dropped in such scenarios1.Reference: =IPS | FortiGate / FortiOS 7.2.3 - Fortinet Documentation

When IPS (Intrusion Prevention System) is configured, if fail-open is 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 5

Question Type: **MultipleChoice**

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)

Options:

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

Answer:

A, B

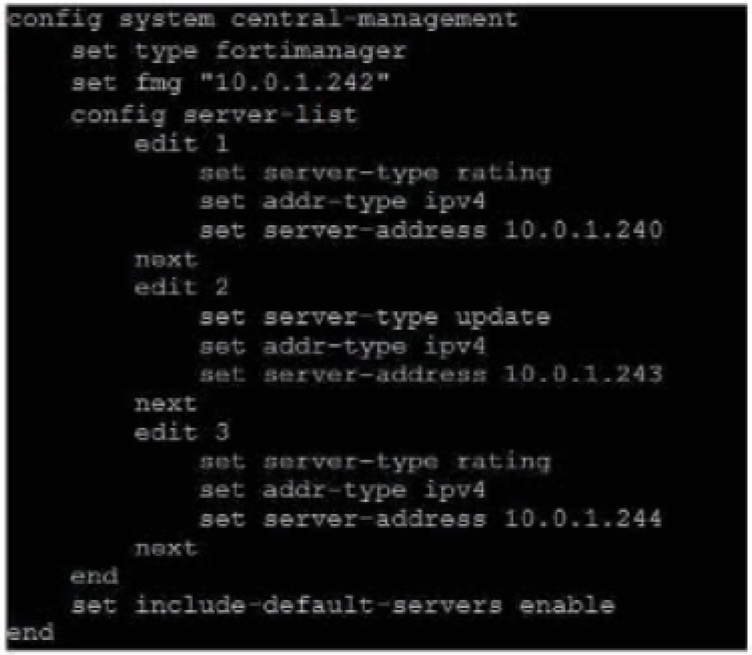
Explanation:

The Virtual Router Redundancy Protocol (VRRP) configuration in the exhibit indicates that 10.1.5.254 is set as the virtual IP (VRIP), commonly serving as the default gateway for the internal network (A). With vrrp-virtual-mac enabled, both FortiGates would use the same virtual MAC address, ensuring a seamless transition during failover (B). The VRRP domain does not use the physical MAC address (C), and the priority settings indicate that FortiGate-A would be the primary router by default due to its higher priority (D).

Question 6

Question Type: **MultipleChoice**

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?

Options:

A- Public FortiGuard servers

B- 10.0.1.242

C- 10.0.1.244

D- 10.0.1.243

Answer:

C

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 7

Question Type: **MultipleChoice**

Which statement about network processor (NP) offloading is true?

Options:

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

Answer:

B

Explanation:

Network processors (NPs) are specialized hardware within FortiGate devices that accelerate certain security functions. One of the primary functions of NPs is to provide IPS signature matching (B), allowing for high-speed inspection of traffic against a database of known threat signatures.

Question 8

Question Type: **MultipleChoice**

Which two statements about IKE vision 2 are true? (Choose two.)

Options:

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

Answer:

B, D

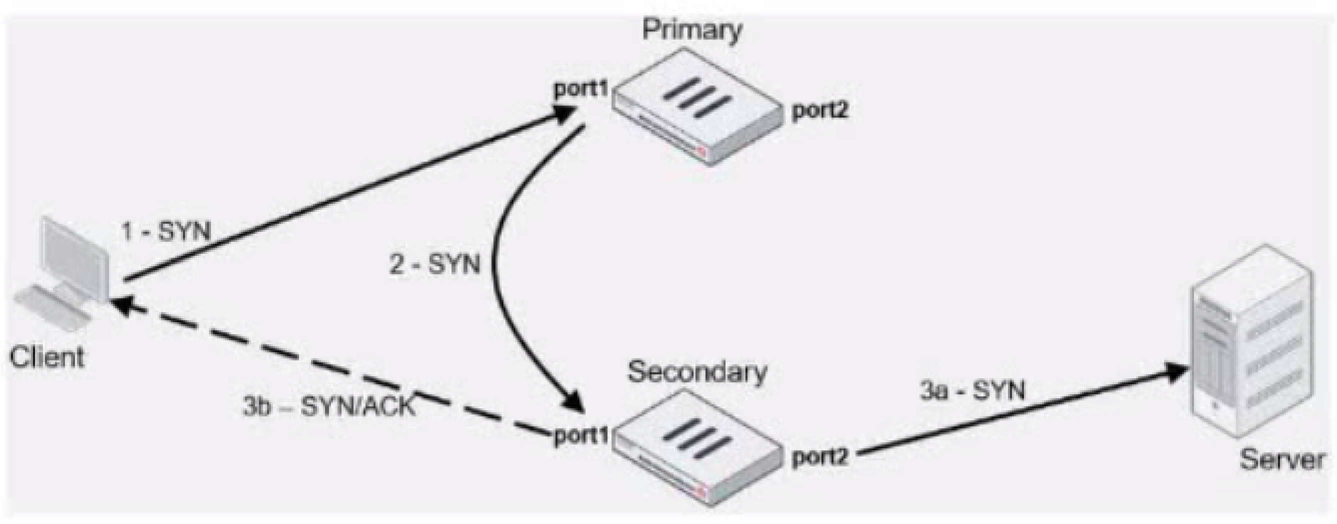
Explanation:

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 9

Question Type: MultipleChoice

Exhibit.



Refer to the exhibit, which contains an active-active toad balancing scenario.

During the traffic flow the primary FortiGate forwards the SYN packet to the secondary FortiGate.

What is the destination MAC address or addresses when packets are forwarded from the primary FortiGate to the secondary FortiGate?

Options:

A- Secondary physical MAC port1

B- Secondary virtual MAC port1

C- Secondary virtual MAC port1 then physical MAC port1

D- Secondary physical MAC port2 then virtual MAC port2

Answer:

A

Explanation:

In an active-active load balancing scenario, when the primary FortiGate forwards the SYN packet to the secondary FortiGate, the destination MAC address would be the secondary's physical MAC on port1, as the packet is being sent over the network and the physical MAC is used for layer 2 transmissions.

Question 10

Question Type: **MultipleChoice**

Which configuration can be used to reduce the number of BGP sessions in on IBGP network?

Options:

A- Route-reflector-peer enable

B- Route-reflector-client enable

C- Route-reflector enable

D- Route-reflector-server enable

Answer:

B

Explanation:

To reduce the number of BGP sessions in an IBGP network, you can use a route reflector, which acts as a focal point for IBGP sessions and readvertises the prefixes to all other peers. To configure a route reflector, you need to enable the route-reflector-client option on the neighbor-group settings of the hub device. This will make the hub device act as a route reflector server and the other devices as route reflector clients.Reference:=Route exchange | FortiGate / FortiOS 7.2.0 - Fortinet Documentation

Question 11

Question Type: MultipleChoice

Which FortiGate in a Security I auric sends togs to FortiAnalyzer?

Options:

A- Only the root FortiGate.

B- Each FortiGate in the Security fabric.

C- The FortiGate devices performing network address translation (NAT) or unified threat management (UTM). if configured.

D- Only the last FortiGate that handled a session in the Security Fabric

Answer:

B

Explanation:

Option B is correct because each FortiGate in the Security Fabric can send logs to FortiAnalyzer for centralized logging and analysis12. This allows you to monitor and manage the entire Security Fabric from a single console and view aggregated reports and dashboards.

Option A is incorrect because the root FortiGate is not the only device that can send logs to FortiAnalyzer.The root FortiGate is the device that initiates the Security Fabric and acts as the central point of contact for other FortiGate devices3. However, it does not have to be the only log source for FortiAnalyzer.

Option C is incorrect because the FortiGate devices performing NAT or UTM are not the only devices that can send logs to FortiAnalyzer.These devices can perform additional security functions on the traffic that passes through them, such as firewall, antivirus, web filtering, etc4. However, they are not the only devices that generate logs in the Security Fabric.

Option D is incorrect because the last FortiGate that handled a session in the Security Fabric is not the only device that can send logs to FortiAnalyzer.The last FortiGate is the device that terminates the session and applies the final security policy5. However, it does not have to be the only device that reports the session information to FortiAnalyzer.Reference: =

1: Security Fabric - Fortinet Documentation1

2: FortiAnalyzer Demo6

3: Security Fabric topology

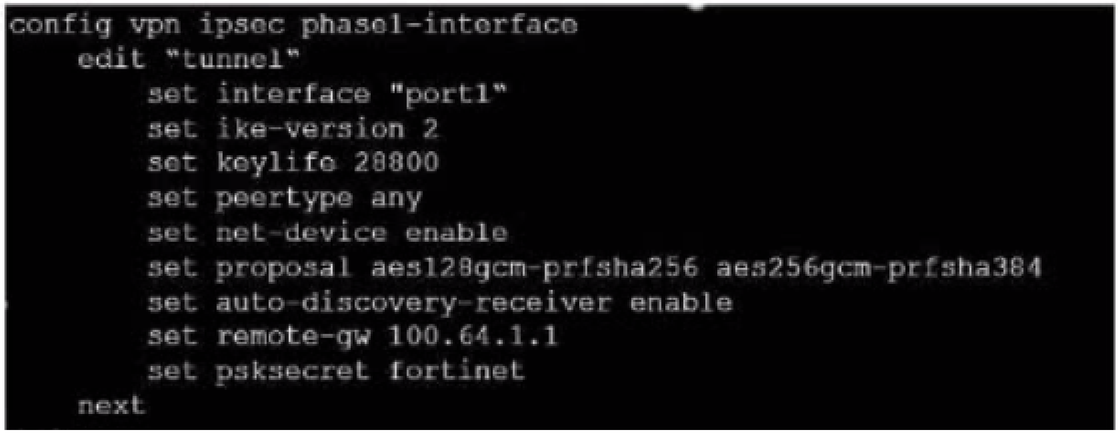
4: Security Fabric UTM features

5: Security Fabric session handling

Question 12

Question Type: **MultipleChoice**

Exhibit.



```
config vpn ipsec phase1-interface
    edit "tunnel"
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device enable
        set proposal aes128gcm-prfsha256 aes256gcm-prfsha384
        set auto-discovery-receiver enable
        set remote-gw 100.64.1.1
        set psksecret fortinet
    next
```

Refer to the exhibit, which contains the partial ADVPN configuration of a spoke.

Which two parameters must you configure on the corresponding single hub? (Choose two.)

Options:

A- Set auto-discovery-sender enable

B- Set ike-version 2

C- Set auto-discovery-forwarder enable

D- Set auto-discovery-receiver enable

Answer:

A, C

Explanation:

For an ADVPN spoke configuration shown, the corresponding hub must have auto-discovery-sender enabled to send shortcut advertisement messages to the spokes. Also, the hub would need to have auto-discovery-forwarder enabled if it is to forward on those shortcut advertisements to other spokes. This allows the hub to inform all spokes about the best path to reach each other. The ike-version does not need to be reconfigured on the hub if it's already set to version 2 and auto-discovery-receiver is not necessary on the hub because it's the one sending the advertisements, not receiving.

FortiOS Handbook - ADVPN