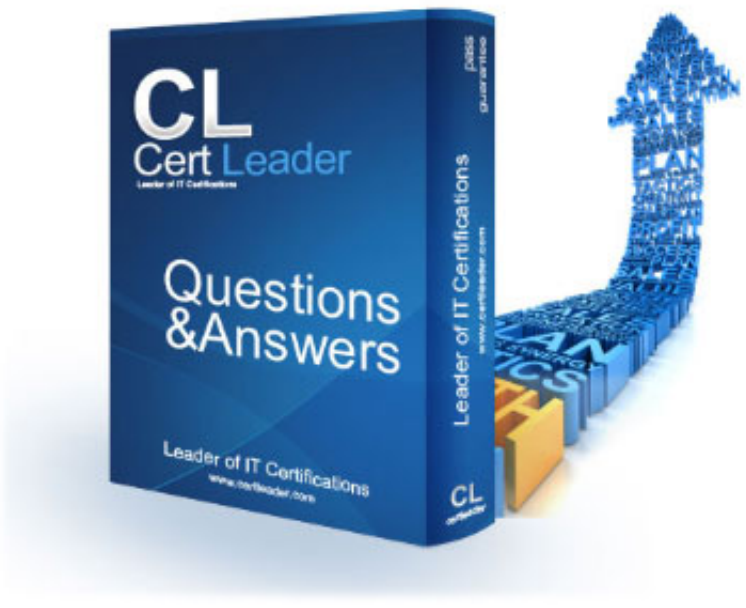
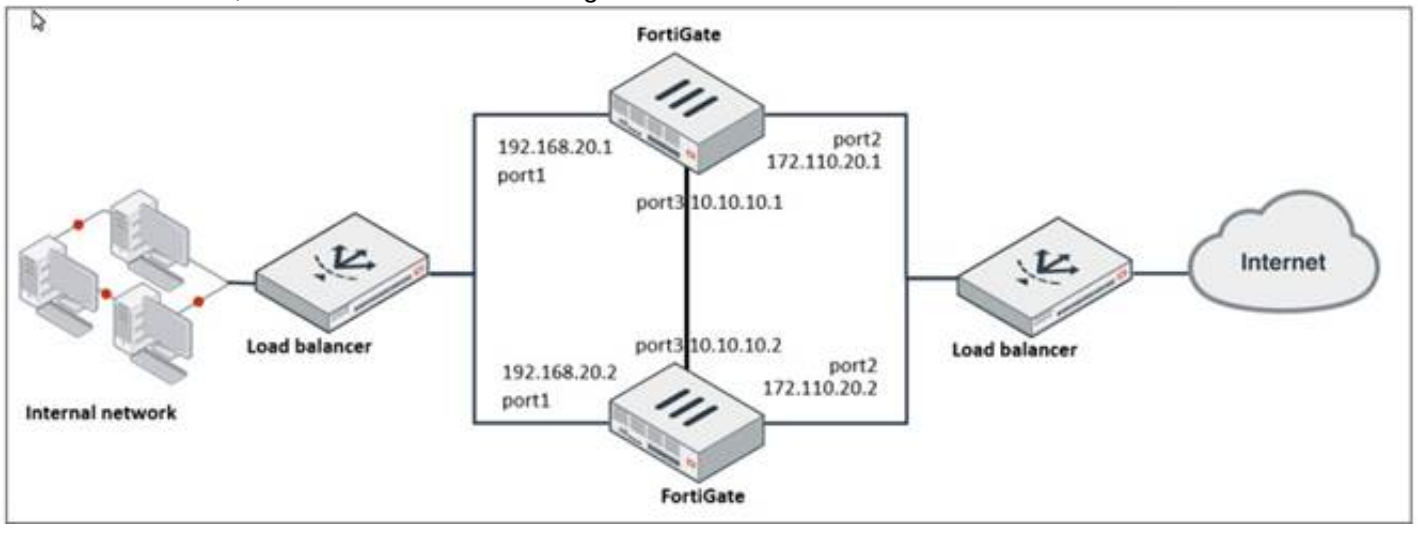
NSE7_EFW-7.2 Dumps

Fortinet NSE 7 - Enterprise Firewall 7.2

https://www.certleader.com/NSE7_EFW-7.2-dumps.html



NEW QUESTION 1
Refer to the exhibit, which shows a network diagram.



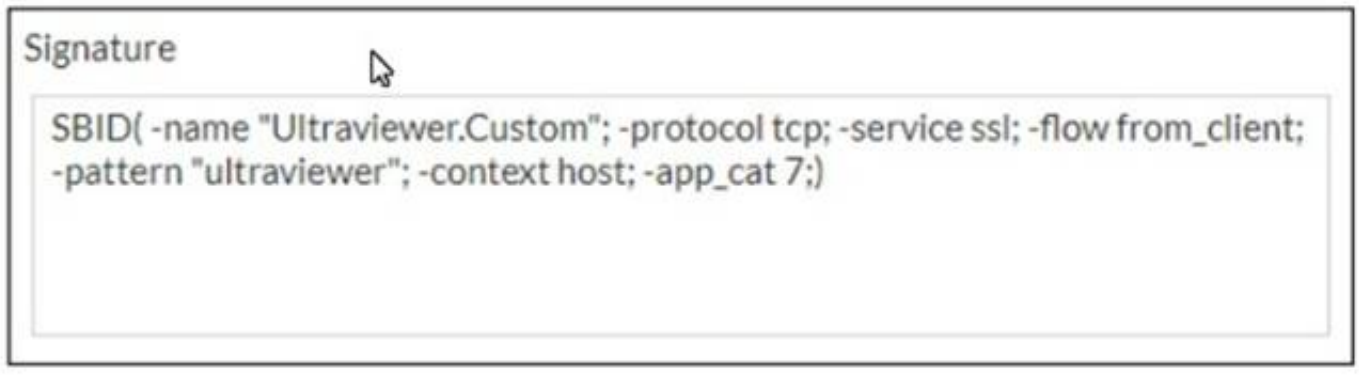
Which protocol should you use to configure the FortiGate cluster?

A. FGCP in active-passive mode
B. OFGSP
C. VRRP
D. FGCP in active-active mode

Answer: A

Explanation:
Given the network diagram and the presence of two FortiGate devices, the Fortinet Gate Clustering Protocol (FGCP) in active-passive mode is the most appropriate for setting up a FortiGate cluster. FGCP supports high availability configurations and is designed to allow one FortiGate to seamlessly take over if the other fails, providing continuous network availability. This is supported by Fortinet documentation for high availability configurations using FGCP.

NEW QUESTION 2
Refer to the exhibit, which shows a custom signature.



Which two modifications must you apply to the configuration of this custom signature so that you can save it on FortiGate? (Choose two.)

A. Add severity.
B. Add attack_id.
C. Ensure that the header syntax is F-SBID.
D. Start options with --.

Answer: AB

Explanation:
For a custom signature to be valid and savable on a FortiGate device, it must include certain mandatory fields. Severity is used to specify the level of threat that the signature represents, and attack_id is a unique identifier for the signature. Without these, the signature would not be complete and could not be correctly utilized by the FortiGate's Intrusion Prevention System (IPS).

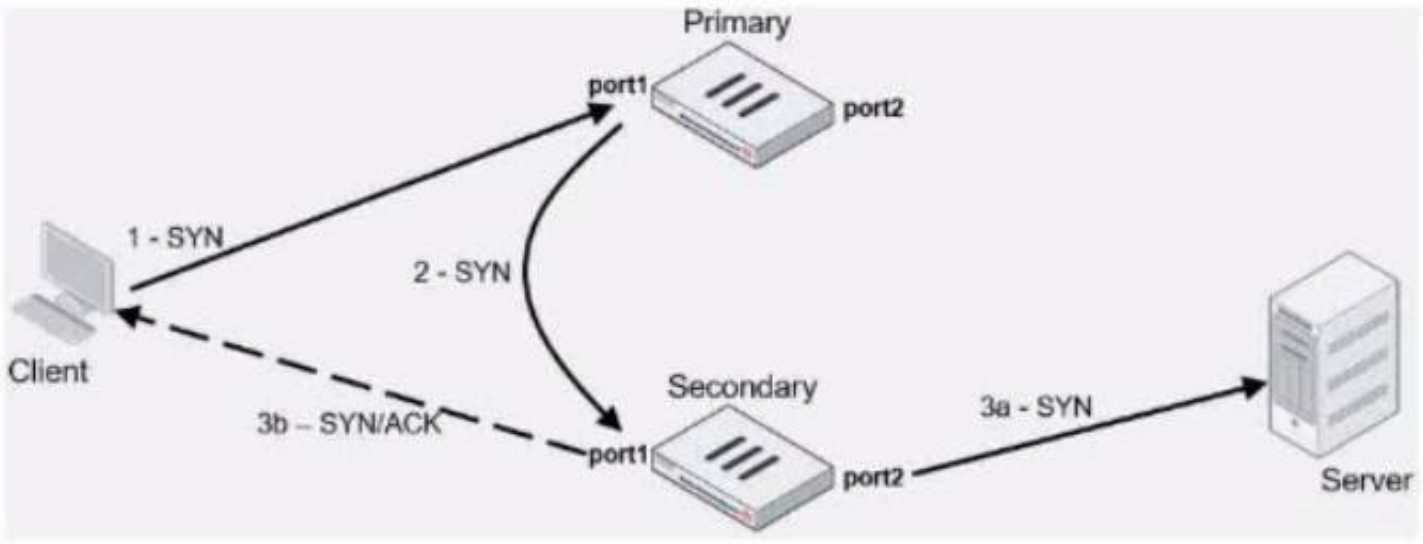
NEW QUESTION 3
Which two statements about the Security fabric are true? (Choose two.)

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

Answer: BC

Explanation:
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

NEW QUESTION 4
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?

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.

NEW QUESTION 5
Exhibit.

```
config vpn ipsec phase1-interface
    edit tunnel
        set type dynamic
        set interface "port1"
        set ike-version 2
        set keylife 28800
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256
        set dpd on-idle
        set add-route enable
        set psksecret fortinet
    next
end
```

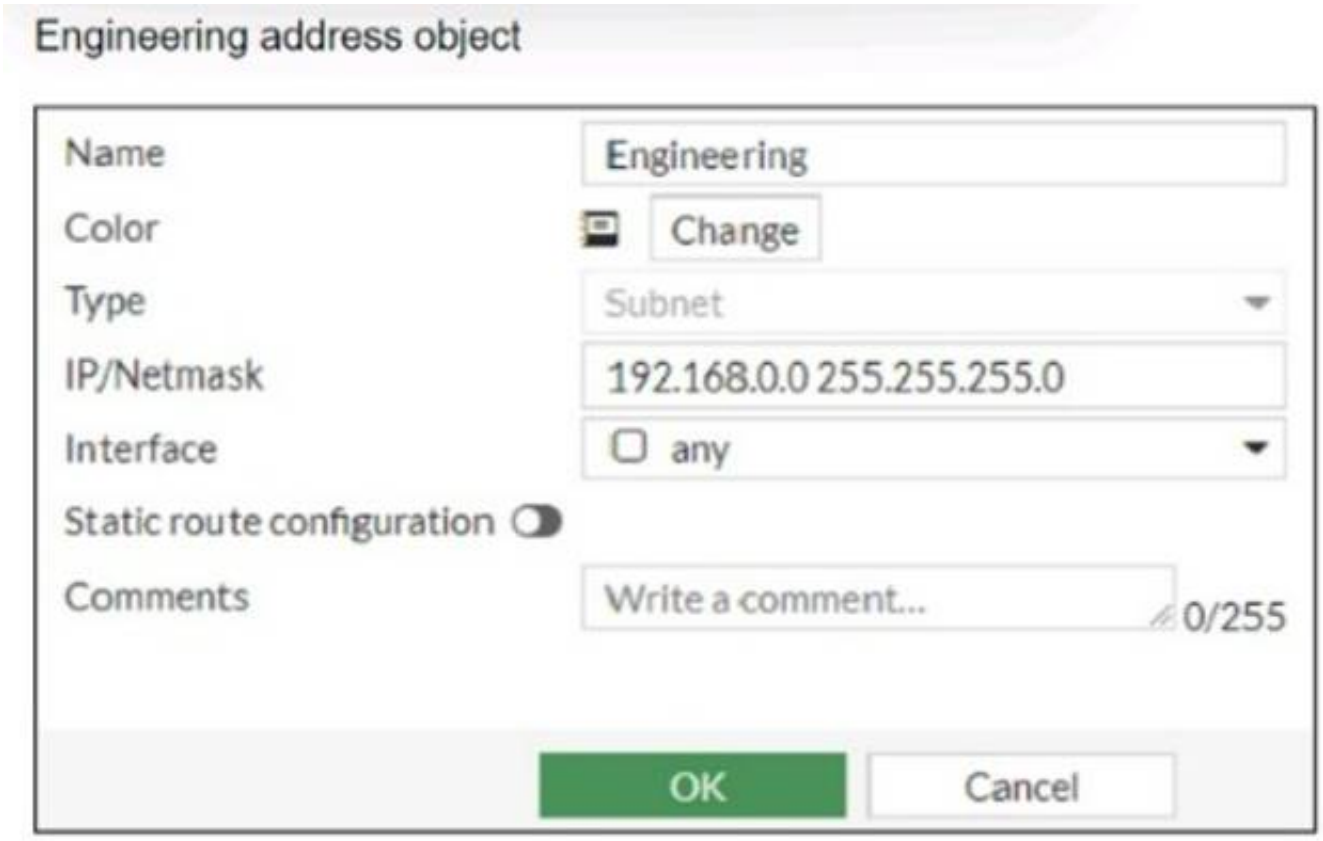
Refer to the exhibit, which contains a partial VPN configuration. What can you conclude from this configuration1?

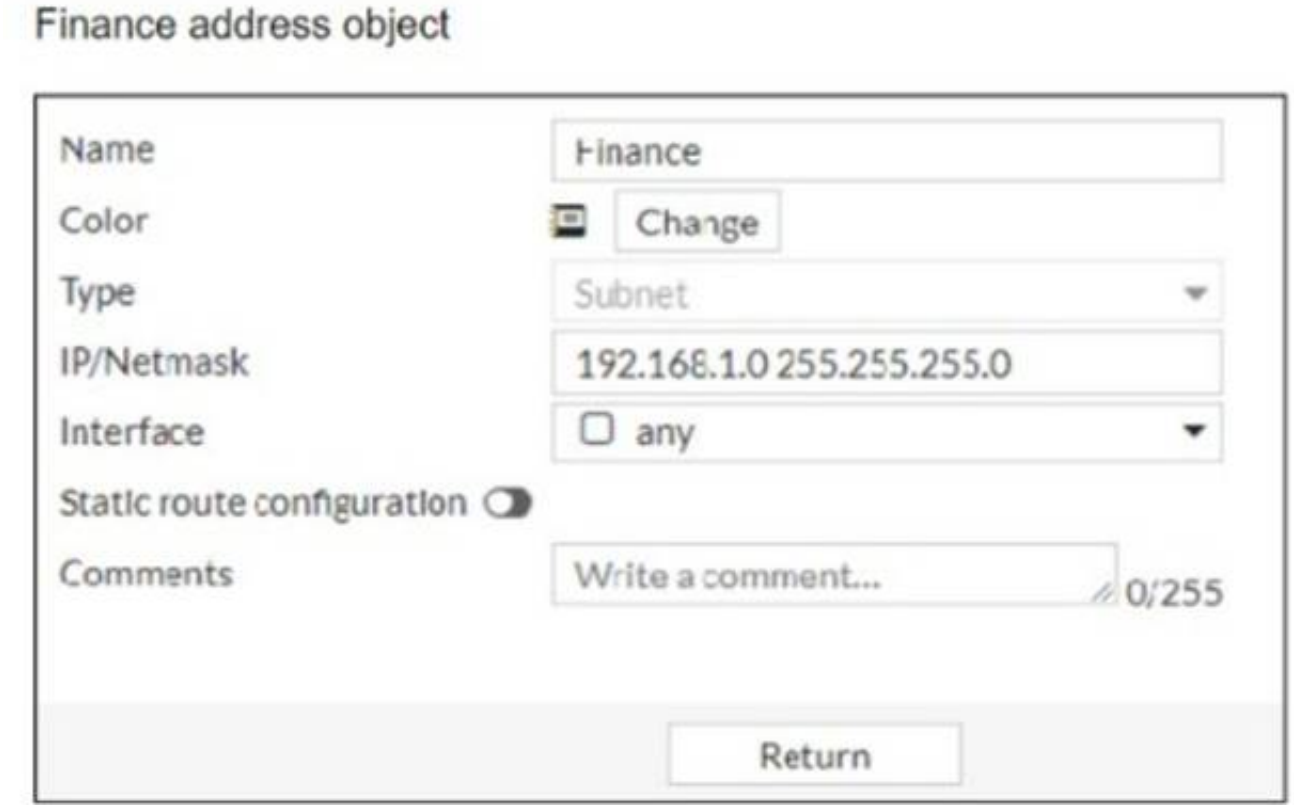
A. FortiGate creates separate virtual interfaces for each dial up client.
B. The VPN should use the dynamic routing protocol to exchange routing information Through the tunnels.
C. Dead peer detection s disabled.
D. The routing table shows a single IPSec virtual interface.

Answer: C

Explanation:
The configuration line “set dpd on-idle” indicates that dead peer detection (DPD) is set to trigger only when the tunnel is idle, not actively disabled1. References: FortiGate IPSec VPN User Guide - Fortinet Document Library
From the given VPN configuration, dead peer detection (DPD) is set to 'on-idle', indicating that DPD is enabled and will be used to detect if the other end of the VPN tunnel is still alive when no traffic is detected. Hence, option C is incorrect. The configuration shows the tunnel set to type 'dynamic', which does not create separate virtual interfaces for each dial- up client (A), and it is not specified that dynamic routing will be used (B). Since this is a phase 1 configuration snippet, the routing table aspect (D) cannot be concluded from this alone.

NEW QUESTION 6
Refer to the exhibits, which show the configurations of two address objects from the same FortiGate.





Why can you modify the Engineering address object, but not the Finance address object?

A. You have read-only access.
B. FortiGate joined the Security Fabric and the Finance address object was configured on the root FortiGate.
C. FortiGate is registered on FortiManager.
D. Another user is editing the Finance address object in workspace mode.

Answer: B

Explanation:
The inability to modify the Finance address object while being able to modify the Engineering address object suggests that the Finance object is being managed by a higher authority in the Security Fabric, likely the root FortiGate. When a FortiGate is part of a Security Fabric, address objects and other configurations may be managed centrally.
This aligns with the Fortinet FortiGate documentation on Security Fabric and central management of address objects.

NEW QUESTION 7
Exhibit.

```
# get router info bgp neighbors
VRF 0 neighbor table:
BGP neighbor is 10.2.0.254, remote AS 65100, local AS 65200, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Not directly connected EBGP
  Last read 00:04:40, hold time is 180, keepalive interval is 60 seconds
  Configured hold time is 180, keepalive interval is 60 seconds
  Received 5 messages, 0 notifications, 0 in queue
  Sent 4 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  NLRI treated as withdraw: 0
  Minimum time between advertisement runs is 30 seconds…
```

Refer to the exhibit, which provides information on BGP neighbors. Which can you conclude from this command output?

A. The router are in the number to match the remote peer.
B. You must change the AS number to match the remote peer.
C. BGP is attempting to establish a TCP connection with the BGP peer.
D. The bfd configuration to set to enable.

Answer: C

Explanation:
The BGP state is “Idle”, indicating that BGP is attempting to establish a TCP connection with the peer. This is the first state in the BGP finite state machine, and it means that no TCP connection has been established yet. If the TCP connection fails, the BGP state will reset to either active or idle, depending on the configuration. References: You can find more information about BGP states and troubleshooting in the following Fortinet Enterprise Firewall 7.2 documents:
? Troubleshooting BGP
? How BGP works

NEW QUESTION 8
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

Answer: D

Explanation:
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

NEW QUESTION 9
Refer to the exhibit, which shows the output of a BGP summary.

```
FGT # get router info bgp summary
BGP router identifier 0.0.0.117, local AS number 65117
BGP table version is 104
3 BGP AS-PATH entries
0 BGP community entries

Neighbor        V    AS       MsgRcvd MsgSent   TblVer  InQ OutQ   Up/Down   State/PfxRcd
10.125.0.60     4 65060       1698    1756      103       0    0    03:02:49        1
10.127.0.75     4 65075       2206    2250      102       0    0    02:45:55        1
100.64.3.1      4 65501       101     115         0       0    0    never       Active

Total number of neighbors 3
```

What two conclusions can you draw from this BGP summary? (Choose two.)

A. External BGP (EBGP) exchanges routing information.
B. The BGP session with peer 10. 127. 0. 75 is established.
C. The router 100. 64. 3. 1 has the parameter bfd set to enable.
D. The neighbors displayed are linked to a local router with the neighbor-range set to a value of 4.

Answer: AB

Explanation:
The output of the BGP (Border Gateway Protocol) summary shows details about the BGP neighbors of a router, their Autonomous System (AS) numbers, the state of the BGP session, and other metrics like messages received and sent.
From the BGP summary provided:
* A.External BGP (EBGP) exchanges routing information.This conclusion can be inferred because the AS numbers for the neighbors are different from the local AS number (65117), which suggests that these are external connections.
* B.The BGP session with peer 10.127.0.75 is established.This is indicated by the state/prefix received column showing a numeric value (1), which typically means that the session is established and a number of prefixes has been received.

* C.The router 100.64.3.1 has the parameter bfd set to enable.This cannot be concluded directly from the summary without additional context or commands specifically showing
BFD (Bidirectional Forwarding Detection) configuration.
* D.The neighbors displayed are linked to a local router with the neighbor-range set to a value of 4.The neighbor-range concept does not apply here; the value 4 in the 'V' column stands for the BGP version number, which is typically 4.

NEW QUESTION 10
Which configuration can be used to reduce the number of BGP sessions in on IBGP network?

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. References := Route exchange | FortiGate / FortiOS 7.2.0 - Fortinet Documentation

NEW QUESTION 10
Refer to the exhibit, which shows config system central-management information.

```
config system central-management
    set type fortimanager
    set allow-push-firmware disable
    set allow-remote-firmware-upgrade disable
    set fmg "10.1.0.241"
    config server-list
        edit 1
            set server-type update
            set server-address 10.1.0.241
        next
    end
    set include-default-servers disable
end
```

Which setting must you configure for the web filtering feature to function?

A. Add serve
B. fortiguar
C. net to the server list.
D. Configure securewf.fortiguar
E. net on the default servers.
F. Set update-server-location to automatic.
G. Configure server-type with the rating option.

Answer: D

Explanation:
For the web filtering feature to function effectively, the FortiGate device
needs to have a server configured for rating services. The rating option in the server-type setting specifies that the server is used for URL rating lookup, which is essential for web filtering. The displayed configuration does not list any FortiGuard web filtering servers, which would be necessary for web filtering. The setting set include-default-servers disable indicates that the default FortiGuard servers are not being used, and hence, a specific server for web filtering (like securewf.fortiguard.net) needs to be configured.

NEW QUESTION 11
Which FortiGate in a Security I auric sends togs to FortiAnalyzer?

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. References: =
? 1: Security Fabric - Fortinet Documentation1
? 2: FortiAnalyzer Demo6
? 3: Security Fabric topology
? 4: Security Fabric UTM features
? 5: Security Fabric session handling

NEW QUESTION 12
Exhibit.

Refer to the exhibit, which contains a partial policy configuration. Which setting must you configure to allow SSH?

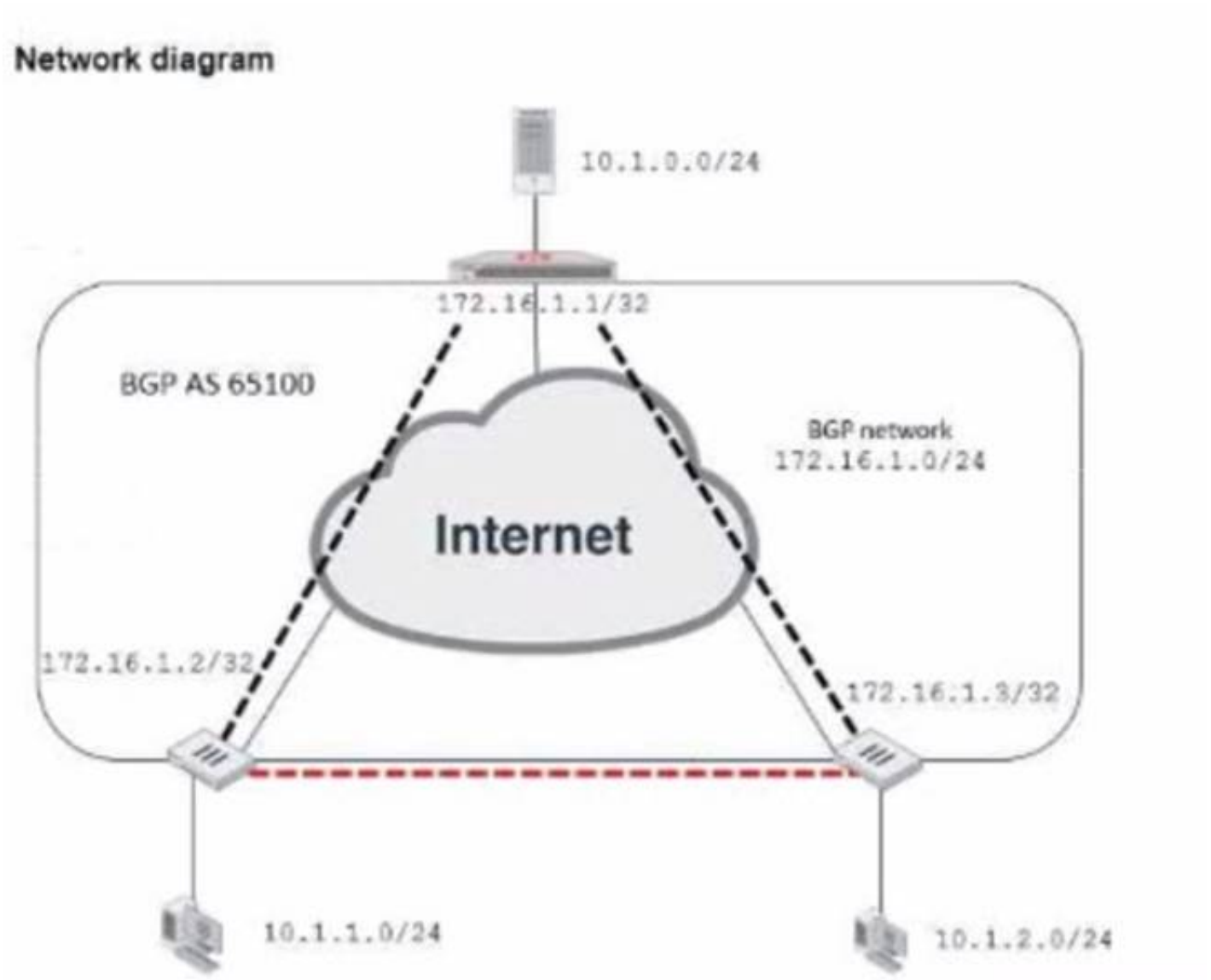
A. Specify SSH in the Service field
B. Configure pot 22 in the Protocol Options field.
C. Include SSH in the Application field
D. Select an application control profile corresponding to SSH in the Security Profiles section

Answer: A

Explanation:
? Option A is correct because to allow SSH, you need to specify SSH in the Service field of the policy configuration. This is because the Service field determines which types of traffic are allowed by the policy1. By default, the Service field is set to App Default, which means that the policy will use the default ports defined by the applications. However, SSH is not one of the default applications, so you need to specify it manually or create a custom service for it2.

? Option B is incorrect because configuring port 22 in the Protocol Options field is not enough to allow SSH. The Protocol Options field allows you to customize the protocol inspection and anomaly protection settings for the policy3. However, this field does not override the Service field, which still needs to match the traffic type.
? Option C is incorrect because including SSH in the Application field is not enough to allow SSH. The Application field allows you to filter the traffic based on the application signatures and categories4. However, this field does not override the Service field, which still needs to match the traffic type.
? Option D is incorrect because selecting an application control profile corresponding to SSH in the Security Profiles section is not enough to allow SSH. The Security Profiles section allows you to apply various security features to the traffic, such as antivirus, web filtering, IPS, etc. However, this section does not override the Service field, which still needs to match the traffic type. References: =
? 1: Firewall policies
? 2: Services
? 3: Protocol options profiles
? 4: Application control

NEW QUESTION 13
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.)

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: AC

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.

NEW QUESTION 17
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE7_EFW-7.2 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE7_EFW-7.2-dumps.html