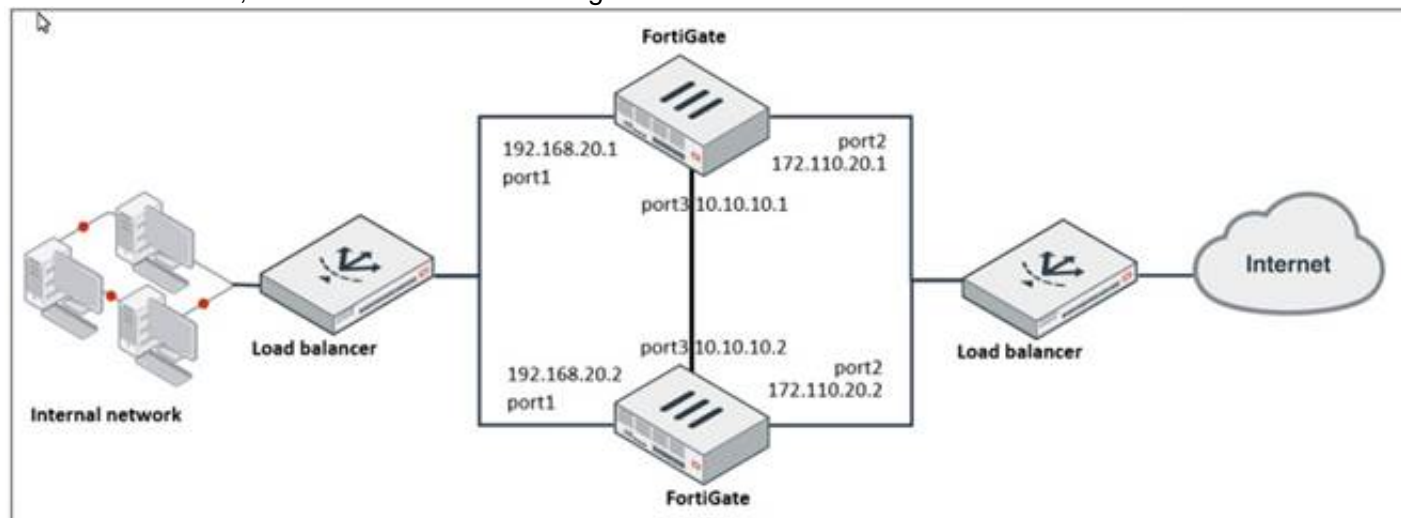# Fortinet

Exam Questions NSE7_EFW-7.2

Fortinet NSE 7 - Enterprise Firewall 7.2

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

Which two statements about bfd are true? (Choose two)

A. It can support neighbor only over the next hop in BGP
B. You can disable it at the protocol level
C. It works for OSPF and BGP
D. You must configure n globally only

Answer: BC

Explanation:

BFD (Bidirectional Forwarding Detection) is a protocol that can quickly detect failures in the forwarding path between two adjacent devices. You can disable BFD at the protocol level by using the "set bfd disable" command under the OSPF or BGP configuration. BFD works for both OSPF and BGP protocols, as well as static routes and SD-WAN rules. References := BFD | FortiGate / FortiOS 7.2.0 - Fortinet Document Library, section "BFD".

NEW QUESTION 3

Which two statements about the neighbor-group command are true? (Choose two.)

A. You can configure it on the GUI.
B. It applies common settings in an OSPF area.
C. It is combined with the neighbor-range parameter.
D. You can apply it in Internal BGP (IBGP) and External BGP (EBGP).

Answer: BD

Explanation:

The neighbor-group command in FortiOS allows for the application of common settings to a group of neighbors in OSPF, and can also be used to simplify configuration by applying common settings to both IBGP and EBGP neighbors. This grouping functionality is a part of the FortiOS CLI and is documented in the Fortinet CLI reference.

NEW QUESTION 4

Winch two statements about ADVPN are true? (Choose two)

A. auto-discovery receiver must be set to enable on the Spokes.
B. Spoke to-spoke traffic never goes through the hub
C. It supports NAI for on-demand tunnels
D. Routing is configured by enabling add-advpn-route

Answer: AC

Explanation:

ADVPN (Auto Discovery VPN) is a feature that allows to dynamically establish direct tunnels (called shortcuts) between the spokes of a traditional Hub and Spoke architecture. The auto-discovery receiver must be set to enable on the spokes to allow them to receive NHRP messages from the hub and other spokes. NHRP (Next Hop Resolution Protocol) is used for on-demand tunnels, which are established when there is traffic between spokes. Routing is configured by enabling add-nhrp-route, not add-advpn- route. References := ADVPN | FortiGate / FortiOS 7.2.0 | Fortinet Document Library, Technical Tip: Fortinet Auto Discovery VPN (ADVPN)

NEW 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

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 6
Refer to the exhibit, which shows a network diagram.
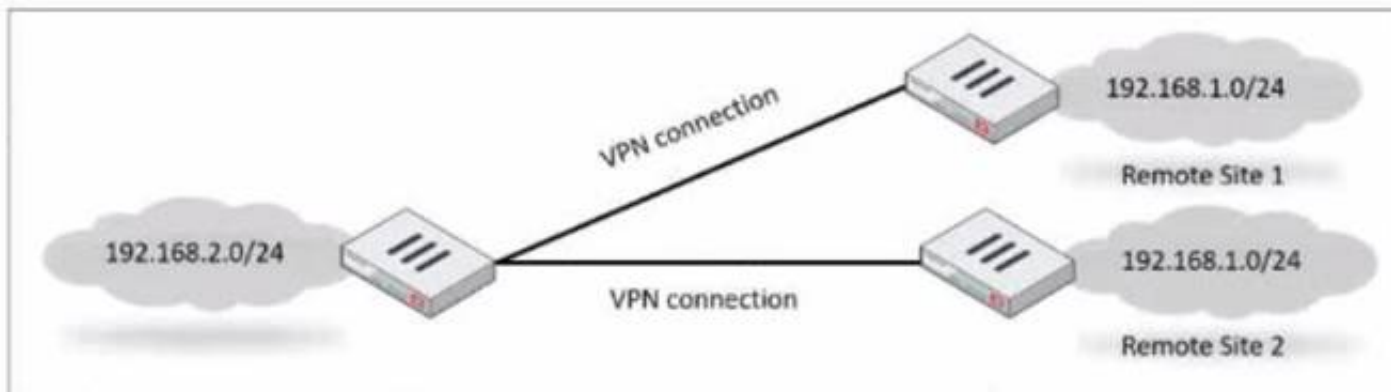
Which IPsec phase 2 configuration should you impalement so that only one remote site is connected at any time?

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 useroute-overlapwith 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).
References:
? FortiOS Handbook - IPsec VPN

NEW QUESTION 7
Exhibit.
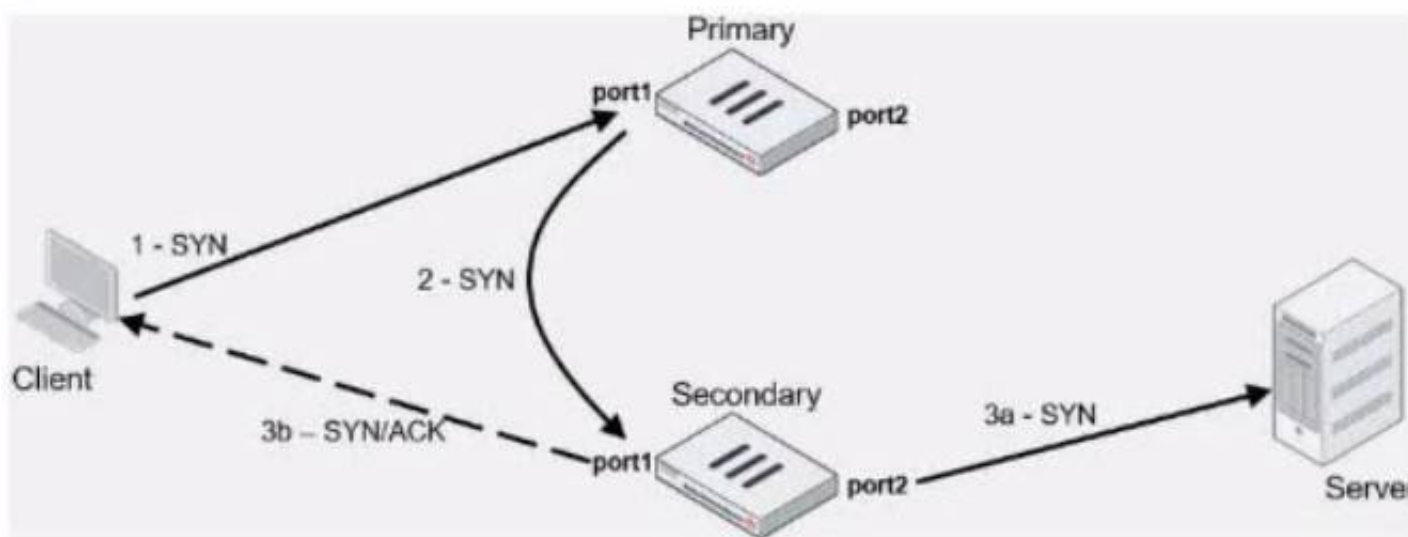
Refer to the exhibit, which contains an active-active toad balancing scenario.
During the traffic flow the primary FortiGate forwards the SYN packet to the secondary VPN FortiGate.
What is the destination MAC address or addresses when packets are forwarded from the primary FortiGate to the secondary 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

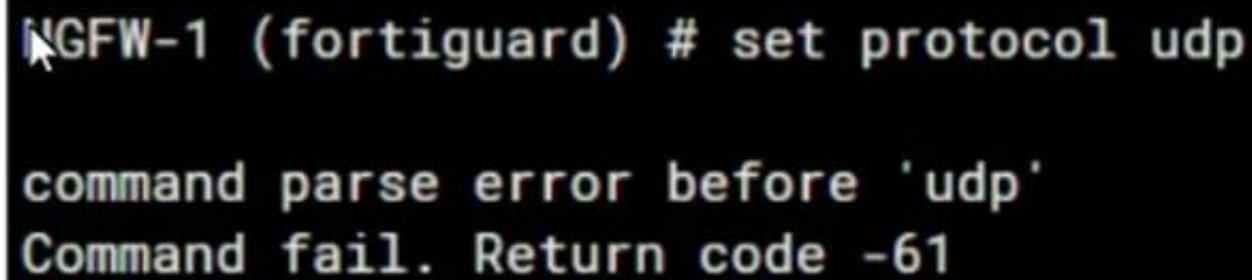**Answer:** A

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 8
Refer to the exhibit, which shows an error in system fortiguard configuration.

```
NGFW-1 (fortiguard) # set protocol udp

command parse error before 'udp'
Command fail. Return code -61
```

What is the reason you cannot set the protocol to udp in config system fortiguard?

A. FortiManager provides FortiGuard.
B. fortiguard-anycast is set to enable.
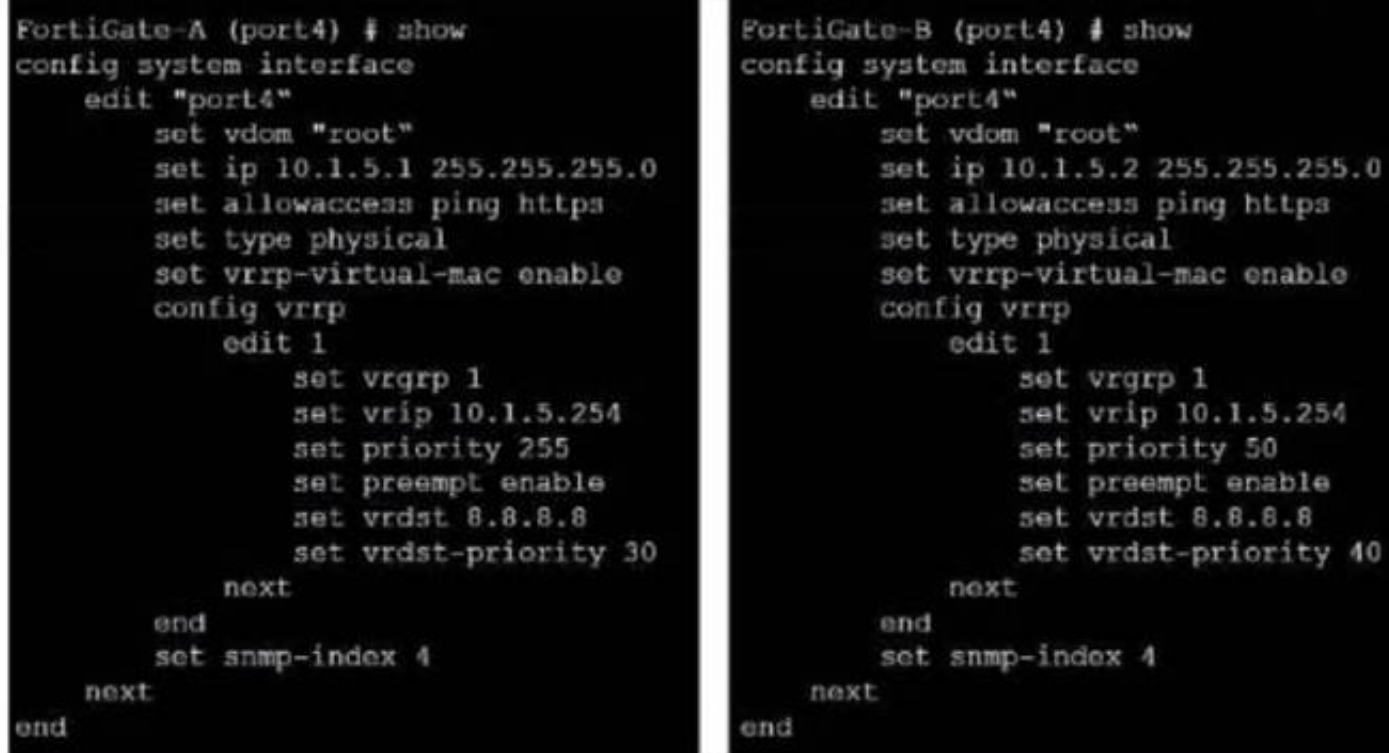C. You do not have the corresponding write access.
D. udp is not a protocol option.

Answer: D

Explanation:
The reason for the command failure when trying to set the protocol to UDP in theconfig system fortiguardis likely that UDP is not a protocol option in this context. The command syntax might be incorrect or the option to set a protocol for FortiGuard updates might not exist in this manner. So the correct answer is D. udp is not a protocol option.

NEW QUESTION 9
Exhibit.

```
FortiGate-A (port4) # show          FortiGate-B (port4) # show
config system interface              config system interface
    edit "port4"                         edit "port4"
        set vdom "root"                      set vdom "root"
        set ip 10.1.5.1 255.255.255.0        set ip 10.1.5.2 255.255.255.0
        set allowaccess ping https           set allowaccess ping https
        set type physical                    set type physical
        set vrrp-virtual-mac enable          set vrrp-virtual-mac enable
        config vrrp                          config vrrp
            edit 1                               edit 1
                set vrgrp 1                          set vrgrp 1
                set vrip 10.1.5.254                  set vrip 10.1.5.254
                set priority 255                     set priority 50
                set preempt enable                   set preempt enable
                set vrdst 8.8.8.8                     set vrdst 8.8.8.8
                set vrdst-priority 30                set vrdst-priority 40
            next                                 next
        end                                  end
        set snmp-index 4                     set snmp-index 4
    next                                 next
end                                  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)

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: AB

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). Withvrrp-virtual-macenabled, 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).

NEW QUESTION 10
Which two statements about the BFD parameter in BGP are true? (Choose two.)

A. It allows failure detection in less than one second.
B. The two routers must be connected to the same subnet.
C. It is supported for neighbors over multiple hops.
D. It detects only two-way failures.

Answer: AC

Explanation:
Bidirectional Forwarding Detection (BFD) is a rapid protocol for detecting failures in the forwarding path between two adjacent routers, including interfaces, data links, and forwarding planes. BFD is designed to detect forwarding path failures in a very short amount of time, often less than one second, which is significantly faster than traditional failure detection mechanisms like hold-down timers in routing protocols.
Fortinet supports BFD for BGP, and it can be used over multiple hops, which allows the detection of failures even if the BGP peers are not directly connected. This functionality enhances the ability to maintain stable BGP sessions over a wider network topology and is documented in Fortinet's guides.

NEW QUESTION 10
You want to configure faster failure detection for BGP
Which parameter should you enable on both connected FortiGate devices?

A. Ebgp-enforce-multihop
B. bfd
C. Distribute-list-in
D. Graceful-restart

Answer: B

Explanation:
BFD (Bidirectional Forwarding Detection) is a protocol that provides fast failure detection for BGP by sending periodic messages to verify the connectivity between two peers1. BFD can be enabled on both connected FortiGate devices by using the command set bfd enable under the BGP configuration2. References: = Technical Tip :
FortiGate BFD implementation and examples …, Configure BGP | FortiGate / FortiOS 7.0.2
- Fortinet Documentation

NEW QUESTION 11
Which ADVPN configuration must be configured using a script on fortiManager, when using VPN Manager to manage fortiGate VPN tunnels?

A. Enable AD-VPN in IPsec phase 1
B. Disable add-route on hub
C. Configure IP addresses on IPsec virtual interlaces
D. Set protected network to all

Answer: A

Explanation:
To enable AD-VPN, you need to edit an SD-WAN overlay template and enable the Auto-Discovery VPN toggle. This will automatically add the required settings to the IPsec template and the BGP template. You cannot enable AD-VPN directly in the IPsec phase 1 settings using VPN Manager. References := ADVPN | FortiManager 7.2.0 - Fortinet Documentation

NEW QUESTION 13
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 15
Which two statements about ADVPN are true? (Choose two.)

A. You must disable add-route in the hub.
B. AllFortiGate devices must be in the same autonomous system (AS).
C. The hub adds routes based on IKE negotiations.
D. You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0.

Answer: CD

Explanation:
C. The hub adds routes based on IKE negotiations: This is part of the ADVPN functionality where the hub learns about the networks behind the spokes and can add routes dynamically based on the IKE negotiations with the spokes.
* D. You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0: This wildcard
setting in the phase 2 selectors allows any-to-any tunnel establishment, which is necessary for the dynamic creation of spoke-to-spoke tunnels.
These configurations are outlined in Fortinet's documentation for setting up ADVPN, where the hub's role in route control and the use of wildcard selectors for phase 2 are emphasized to enable dynamic tunneling betwen spokes.

NEW QUESTION 19
Which statement about network processor (NP) offloading is true?

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.

NEW QUESTION 24
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?

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. References := Fortinet Enterprise Firewall Study Guide for FortiOS 7.2, page 132.

NEW QUESTION 25
Exhibit.
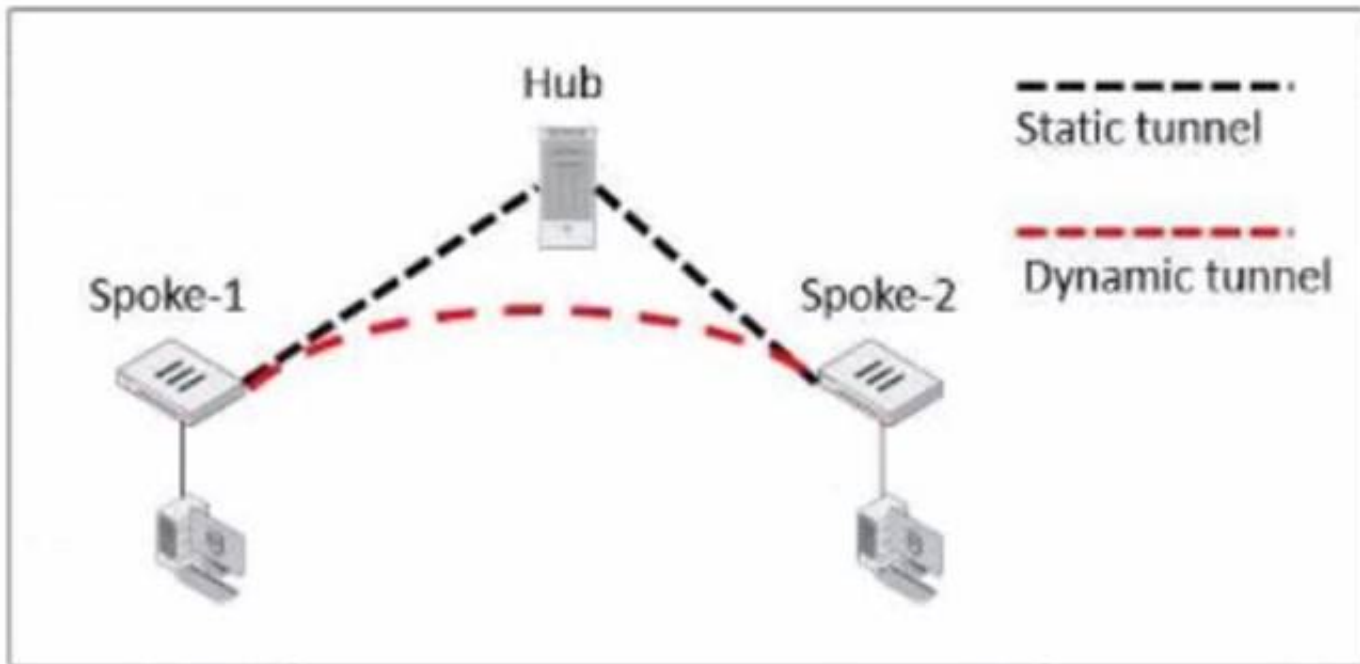
Refer to the exhibit, which shows an ADVPN network.
The client behind Spoke-1 generates traffic to the device located behind Spoke-2. Which first message floes the hub send to Spoke-110 bring up the dynamic tunnel?

A. Shortcut query
B. Shortcut reply
C. Shortcut offer
D. Shortcut forward

Answer: A

Explanation:
In an ADVPN scenario, when traffic is initiated from a client behind one spoke to another spoke, the hub sends a shortcut query to the initiating spoke. This query is used to determine if there is a more direct path for the traffic, which can then trigger the establishment of a dynamic tunnel between the spokes.

NEW QUESTION 30
Refer to the exhibit, which contains a partial BGP combination.

You want to configure a loopback as the OGP source.
Which two parameters must you set in the BGP configuration? (Choose two)

A. ebgp-enforce-multihop
B. recursive-next-hop
C. ibgp-enfoce-multihop
D. update-source

Answer: AD

Explanation:
 To configure a loopback as the BGP source, you need to set the "ebgp- enforce-multihop" and "update-source" parameters in the BGP configuration. The "ebgp-enforce-multihop" allows EBGP connections to neighbor routers that are not directly connected, while "update-source" specifies the IP address that should be used for the BGP
session1. References := BGP on loopback, Loopback interface, Technical Tip: Configuring EBGP Multihop Load-Balancing, Technical Tip: BGP routes are not installed in routing
table with loopback as update source

NEW QUESTION 34
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 35
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 38
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 42
Refer to the exhibit, which contains a partial OSPF configuration.

```
config router ospf
    set router-id 0.0.0.3
    set restart-mode graceful-restart
    set restart-period 30
    set restart-on-topology-change enable
    ...
end
```

What can you conclude from this output?

A. Neighbors maintain communication with the restarting router.
B. The router sends grace LSAs before it restarts.
C. FortiGate restarts if the topology changes.
D. The restarting router sends gratuitous ARP for 30 seconds.

Answer: B

Explanation:
From the partial OSPF (Open Shortest Path First) configuration output:
* B. The router sends grace LSAs before it restarts: This is implied by the command 'set restart-mode graceful-restart'. When OSPF is configured with graceful restart, the router sends grace LSAs (Link State Advertisements) to inform its neighbors that it is restarting, allowing for a seamless transition without recalculating routes.
Fortinet documentation on OSPF configuration clearly states that enabling graceful restart mode allows the router to maintain its adjacencies and routes during a brief restart period.

NEW QUESTION 45
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.)

A. Set auto-discovery-sender enable
B. Set ike-version 2
C. Set auto-discovery-forwarder enable
D. Set auto-discovery-receiver enable

Answer: AC

Explanation:
For an ADVPN spoke configuration shown, the corresponding hub must have auto-discovery-senderenabled to send shortcut advertisement messages to the spokes. Also, the hub would need to haveauto-discovery-forwarderenabled 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. Theike-versiondoes not need to be reconfigured on the hub if it's already set to version 2 andauto-discovery-receiveris not necessary on the hub because it's the one sending the advertisements, not receiving.
References:
? FortiOS Handbook - ADVPN

NEW QUESTION 46
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE7_EFW-7.2 Practice Exam Features:

* NSE7_EFW-7.2 Questions and Answers Updated Frequently

* NSE7_EFW-7.2 Practice Questions Verified by Expert Senior Certified Staff

* NSE7_EFW-7.2 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE7_EFW-7.2 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE7_EFW-7.2 Practice Test Here](https://www.surepassexam.com/NSE7_EFW-7.2-exam-dumps.html)