Exam Questions NSE7_EFW-7.2

Fortinet NSE 7 - Enterprise Firewall 7.2

https://www.2passeasy.com/dumps/NSE7_EFW-7.2/

NEW QUESTION 1
Exhibit.

```
Routing table for VRF=0
B*      0.0.0.0/0 [20/0] via 100.64.1.254 (recursive is directly connected, port1), 00:03:58, [1/0]
C       10.1.0.0/24 is directly connected, port3
B       10.1.1.0/24 [200/0] via 172.16.1.2 (recursive is directly connected, tunnel_0), 00:03:25, [1/0]
B       10.1.2.0/24 [200/0] via 172.16.1.3 (recursive is directly connected, tunnel_1), 00:03:21, [1/0]
O       10.1.4.0/24 [110/2] via 10.1.0.100, port3, 00:04:56, [1/0]
O       10.1.10.0/24 [110/2] via 10.1.0.1, port3, 00:04:56, [1/0]
C       100.64.1.0/24 is directly connected, port1
C       100.64.2.0/24 is directly connected, port2
C       172.16.1.1/32 is directly connected, tunnel_0
                     is directly connected, tunnel_1
C       172.16.1.2/32 is directly connected, tunnel_0
C       172.16.1.3/32 is directly connected, tunnel_1
C       172.16.100.0/24 is directly connected, port8
```

Refer to the exhibit, which shows a partial touting table
What two concisions can you draw from the corresponding FortiGate configuration? (Choose two.)

A. IPSec Tunnel aggregation is configured
B. net-device is enabled in the tunnel IPSec phase 1 configuration
C. OSPI is configured to run over IPSec.
D. add-route is disabled in the tunnel IPSec phase 1 configuration.

Answer: BD

Explanation:
? Option B is correct because the routing table shows that the tunnel interfaces have a netmask of 255.255.255.255, which indicates that net-device is enabled in the phase 1 configuration. This option allows the FortiGate to use the tunnel interface as a next-hop for routing, without adding a route to the phase 2 destination1.
? Option D is correct because the routing table does not show any routes to the phase 2 destination networks, which indicates that add-route is disabled in the phase 1 configuration. This option controls whether the FortiGate adds a static route to the phase 2 destination network using the tunnel interface as the gateway2.
? Option A is incorrect because IPSec tunnel aggregation is a feature that allows multiple phase 2 selectors to share a single phase 1 tunnel, reducing the number of tunnels and improving performance3. This feature is not related to the routing table or the phase 1 configuration.
? Option C is incorrect because OSPF is a dynamic routing protocol that can run over IPSec tunnels, but it requires additional configuration on the FortiGate and the peer device4. This option is not related to the routing table or the phase 1 configuration. References: =
? 1: Technical Tip: 'set net-device' new route-based IPsec logic2
? 2: Adding a static route5
? 3: IPSec VPN concepts6
? 4: Dynamic routing over IPsec VPN7

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

Signature

SBID(-name "Ultraviewer.Custom"; -protocol tcp; -service ssl; -flow from_client;
-pattern "ultraviewer"; -context host; -app_cat 7;)

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
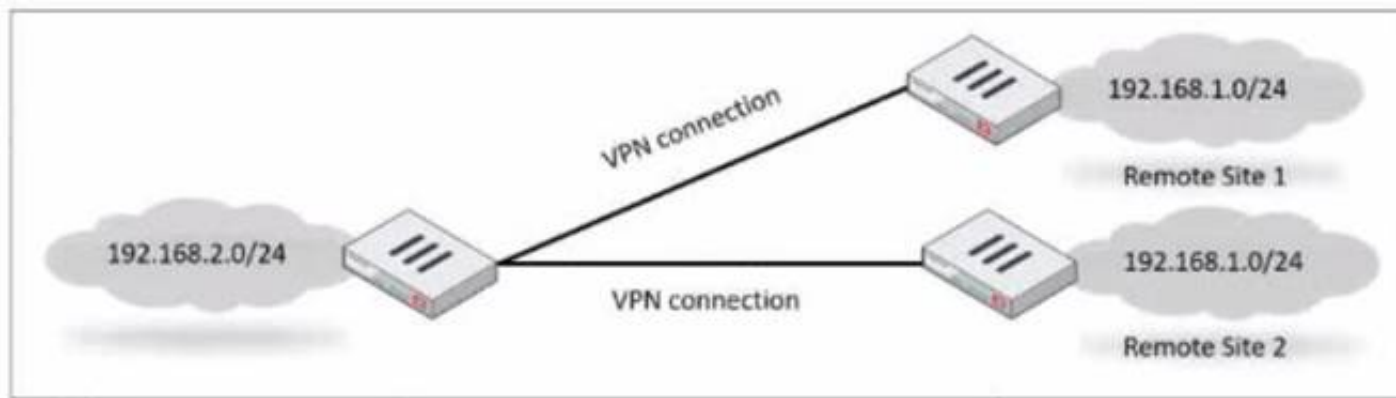
Answer: BC

Explanation:
In the Security Fabric, only the root FortiGate sends logs to FortiAnalyzer (B). Additionally, only FortiGate devices with configuration-sync enabled 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
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 5
You want to block access to the website ww.eicar.org using a custom IPS signature. Which custom IPS signature should you configure?
A)
```
F-SBID( --name "eicar"; --protocol udp; --flow from_server; --pattern "eicar"; --context host;)
```
B)
```
F-SBID( --name "detect_eicar"; --protocol udp; --service ssl; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)
```
C)
```
F-SBID( --name "detect_eicar"; --protocol tcp; --service dns; --flow from_server; --pattern "eicar"; --no_case;)
```
D)
```
F-SBID( --name "eicar"; --protocol tcp; --service HTTP; --flow from_client; --pattern "www.eicar.org"; --no_case; --context host;)
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

Explanation:
 Option D is the correct answer because it specifically blocks access to the website "www.eicar.org" using TCP protocol and HTTP service, which are commonly used for web browsing. The other options either use the wrong protocol (UDP), the wrong service (DNS or SSL), or the wrong pattern ("eicar" instead of "www.eicar.org"). References := Configuring custom signatures | FortiGate / FortiOS 7.4.0 - Fortinet Document Library, section "Signature to block access to example.com".

NEW QUESTION 6
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 7

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

A. Only some IKE version 2 packets are considered fragmentable.
B. The reassembly timeout default value is 30 seconds.
C. It is performed at the IP layer.
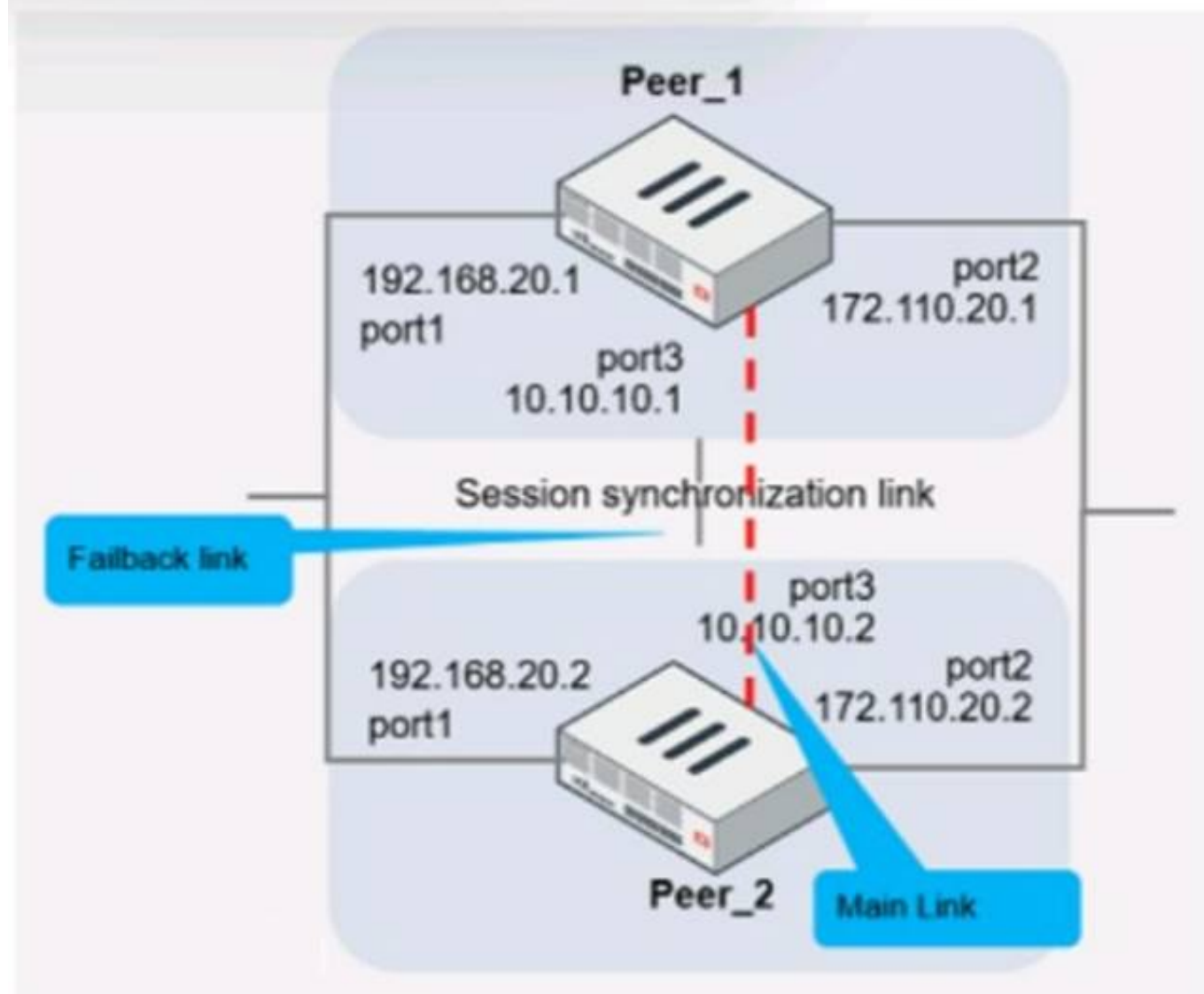D. The maximum number of IKE version 2 fragments is 128.

Answer: AD

Explanation:
In IKE version 2, not all packets are fragmentable. Only certain messages within the IKE negotiation process can be fragmented. Additionally, there is a limit to the number of fragments that IKE version 2 can handle, which is 128. This is specified in the Fortinet documentation and ensures that the IKE negotiation process can proceed even in networks that have issues with large packets. The reassembly timeout and the layer at which fragmentation occurs are not specified in this context within Fortinet documentation.

NEW QUESTION 8
Refer to the exhibit, which shows two configured FortiGate devices and peering over FGSP.

The main link directly connects the two FortiGate devices and is configured using the set
session-syn-dev <interface> command.
What is the primary reason to configure the main link?

A. To have both sessions and configuration synchronization in layer 2
B. To load balance both sessions and configuration synchronization between layer 2 and 3
C. To have only configuration synchronization in layer 3
D. To have both sessions and configuration synchronization in layer 3

Answer: D

Explanation:
The primary purpose of configuring a main link between the devices is to synchronize session information so that if one unit fails, the other can continue processing traffic without dropping active sessions.
* A.To have both sessions and configuration synchronization in layer 2.This is incorrect because FGSP is used for session synchronization, not configuration synchronization. B.To load balance both sessions and configuration synchronization between layer 2 and 3.FGSP does not perform load balancing and is not used for configuration synchronization.
* C.To have only configuration synchronization in layer 3.The main link is not used solely for configuration synchronization.
* D.To have both sessions and configuration synchronization in layer 3.The main link in an FGSP setup is indeed used to synchronize session information across the devices, and it operates at layer 3 since it uses IP addresses to establish the peering.

NEW QUESTION 9
Which two statements about metadata variables are true? (Choose two.)

A. You create them on FortiGate
B. They apply only to non-firewall objects.
C. The metadata format is $<metadata_variabie_name>.
D. They can be used as variables in scripts

Answer: AD

Explanation:
Metadata variables in FortiGate are created to store metadata associated
with different FortiGate features. These variables can be used in various configurations and scripts to dynamically replace the variable with its actual value during processing. A: You create metadata variables on FortiGate. They are used to store metadata for FortiGate features and can be called upon in different configurations. D: They can be used as variables in scripts. Metadata variables are utilized within the scripts to dynamically insert values as per the context when the script runs.
Fortinet FortiOS Handbook: CLI Reference

NEW QUESTION 10
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.
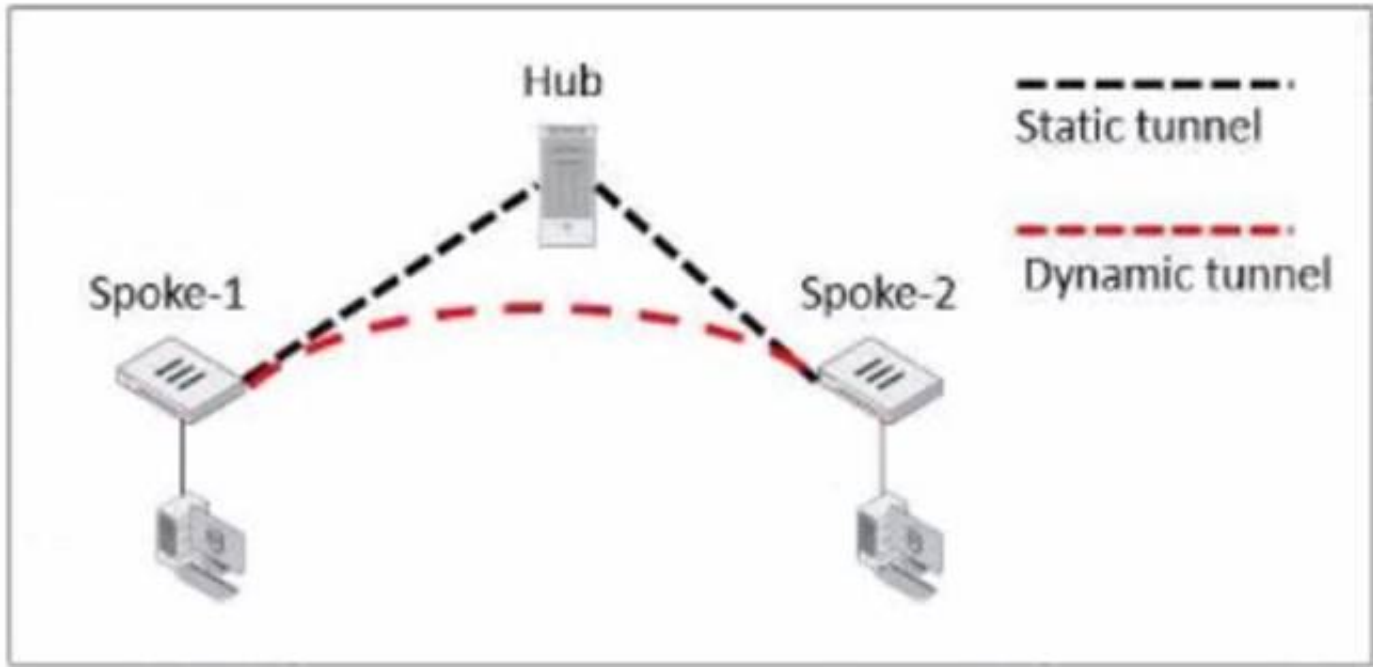D. You must configure phase 2 quick mode selectors to 0.0.0.0 0.0.0.0.

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 10
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 13
Refer to the exhibit, which shows a routing table.

Network ≑	Gateway IP ≑	Interfaces ≑	Distance ≑	Type ≑
0.0.0.0/0	10.1.0.254	port1	10	Static
10.1.0.0/24	0.0.0.0	port1	0	Connected
10.1.4.0/24	10.1.0.100	port1	110	OSPF
10.1.10.0/24	0.0.0.0	port2	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

What two options can you configure in OSPF to block the advertisement of the 10.1.10.0 prefix? (Choose two.)

A. Remove the 16.1.10.C prefix from the OSPF network
B. Configure a distribute-list-out
C. Configure a route-map out
D. Disable Redistribute Connected

Answer: BC

Explanation:
To block the advertisement of the 10.1.10.0 prefix in OSPF, you can configure a distribute-list-out or a route-map out. A distribute-list-out is used to filter outgoing routing updates from being advertised to OSPF neighbors1. A route-map out can also be used for filtering and is applied to outbound routing updates2. References := Technical Tip: Inbound route filtering in OSPF usi … - Fortinet Community, OSPF | FortiGate / FortiOS 7.2.2 - Fortinet Documentation

NEW QUESTION 17
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 19
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 22
You contoured an address object on the tool fortiGate in a Security Fabric. This object is not synchronized with a downstream device. Which two reasons could be the cause? (Choose two)

A. The address object on the tool FortiGate has fabric-object set to disable
B. The root FortiGate has configuration-sync set to enable
C. The downstream TortiGate has fabric-object-unification set to local
D. The downstream FortiGate has configuration-sync set to local

Answer: AC

Explanation:
? Option A is correct because the address object on the tool FortiGate will not be synchronized with the downstream devices if it has fabric-object set to disable. This option controls whether the address object is shared with other FortiGate devices in the Security Fabric or not1.
? Option C is correct because the downstream FortiGate will not receive the address object from the tool FortiGate if it has fabric-object-unification set to local. This option controls whether the downstream FortiGate uses the address objects from the root FortiGate or its own local address objects2.
? Option B is incorrect because the root FortiGate has configuration-sync set to enable by default, which means that it will synchronize the address objects with the downstream devices unless they are disabled by the fabric-object option3.
? Option D is incorrect because the downstream FortiGate has configuration-sync set to local by default, which means that it will receive the address objects from the root FortiGate unless they are overridden by the fabric-object-unification
option4. References: =
? 1: Group address objects synchronized from FortiManager5
? 2: Security Fabric address object unification6
? 3: Configuration synchronization7
? 4: Configuration synchronization7
? : Security Fabric - Fortinet Documentation

NEW QUESTION 26
You want to improve reliability over a lossy IPSec tunnel.
Which combination of IPSec phase 1 parameters should you configure?

A. fec-ingress and fec-egress
B. Odpd and dpd-retryinterval
C. fragmentation and fragmentation-mtu
D. keepalive and keylive

Answer: C

Explanation:
For improving reliability over a lossy IPSec tunnel, the fragmentation and fragmentation-mtu parameters should be configured. In scenarios where there might be

issues with packet size or an unreliable network, setting the IPsec phase 1 to allow for fragmentation will enable large packets to be broken down, preventing them from being dropped due to size or poor network quality. The fragmentation-mtu specifies the size of the fragments. This is aligned with Fortinet's recommendations for handling IPsec VPN over networks with potential packet loss or size limitations.

NEW QUESTION 28
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 30
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE7_EFW-7.2 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE7_EFW-7.2 Product From:

https://www.2passeasy.com/dumps/NSE7_EFW-7.2/

Money Back Guarantee

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