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
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 2
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 applyingcommon 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.

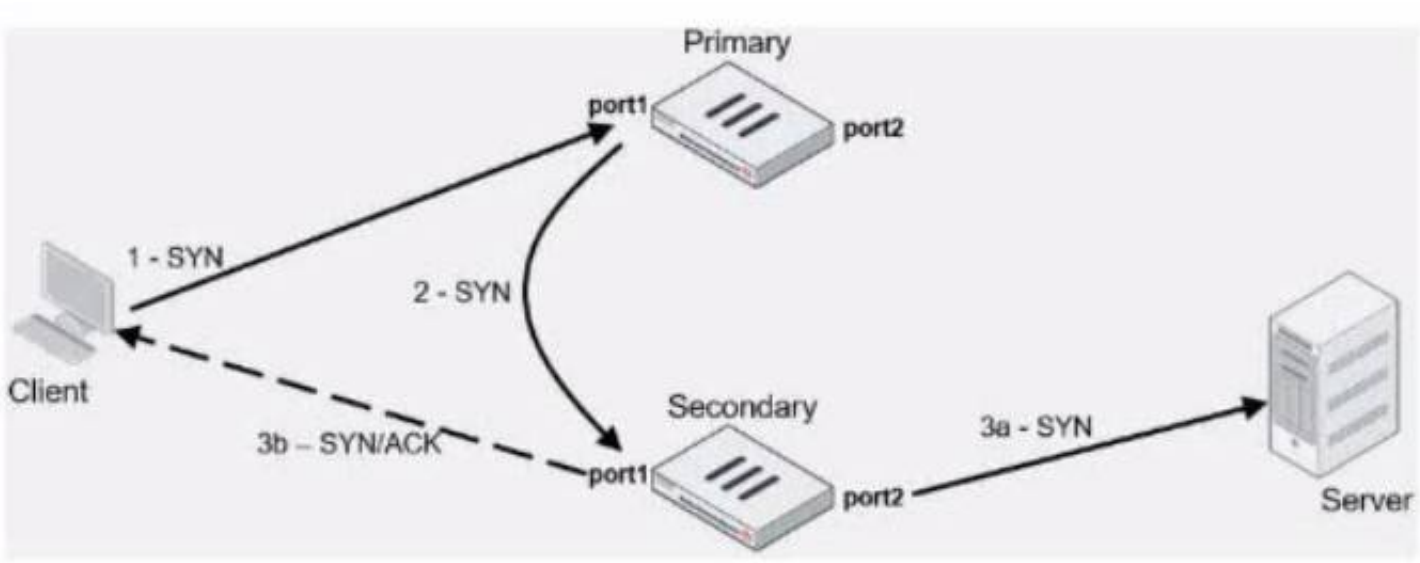
NEW QUESTION 3
Winch two statements about ADVPN are true? (Choose two)

A. auto-discovery receiver must be set to enable on the Spokes.
B. Spoke to-spoke traffic never goes through the hub
C. lt 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 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
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 6
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 7
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 8
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	port3	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 9
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
```

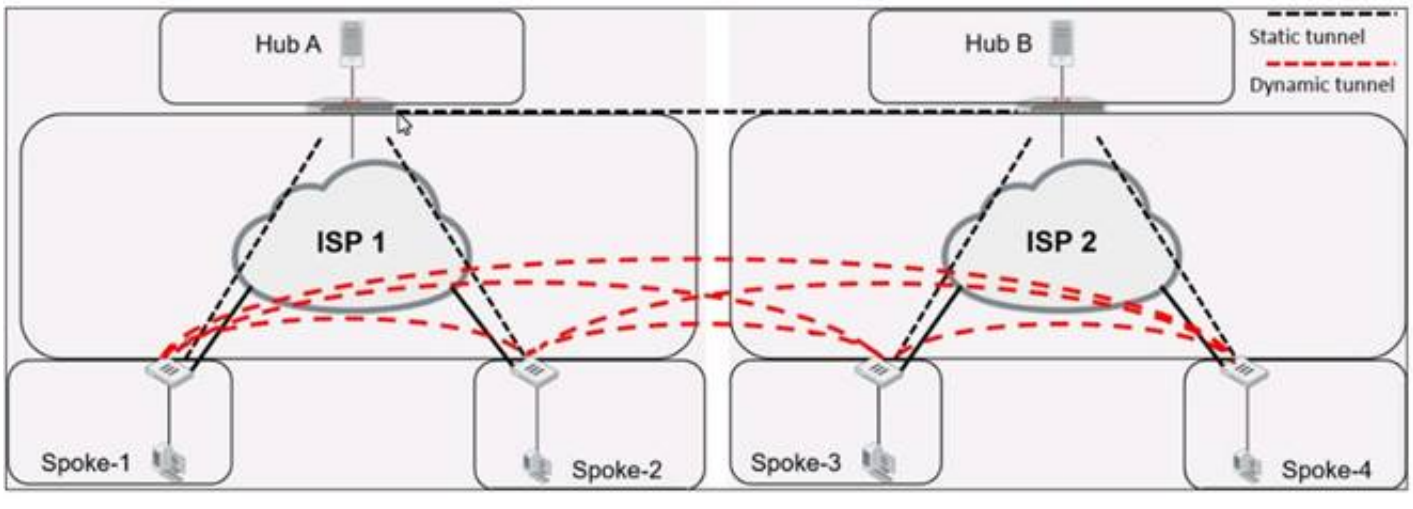
Which setting must you configure for the web filtering feature to function?

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 10
Refer to the exhibit, which shows an ADVPN network.



Which VPN phase 1 parameters must you configure on the hub for the ADVPN feature to function? (Choose two.)

A. set auto-discovery-forwarder enable
B. set add-route enable
C. set auto-discovery-receiver enable
D. set auto-discovery-sender enable

Answer: AC

Explanation:
For the ADVPN feature to function properly on the hub, the following phase 1 parameters must be configured:
* A. set auto-discovery-forwarder enable: This enables the hub to forward shortcut information to the spokes, which is essential for them to establish direct tunnels.
* C. set auto-discovery-receiver enable: This allows the hub to receive shortcut offers from the spokes.
This information is corroborated by the Fortinet documentation, which explains that in an ADVPN setup, the hub must be able to both forward and receive shortcut information for dynamic tunnel creation between spokes.

NEW QUESTION 10
An administrator has configured two fortiGate devices for an HA cluster. While testing HA failover, the administrator notices that some of the switches in the network continue to send traffic to the former primary device What can the administrator do to fix this problem?

A. Verify that the speed and duplex settings match between me FortiGate interfaces andthe connected switch ports
B. Configure set link -failed signal enable under-config system ha on both Cluster members
C. Configure remote link monitoring to detect an issue in the forwarding path
D. Configure set send-garp-on-failover enables under config system ha on both cluster members

Answer: B

Explanation:
Virtual MAC Address and Failover
- The new primary broadcasts Gratuitous ARP packets to notify the network that each virtual MAC is now reachable through a different switch port.
- Some high-end switches might not clear their MAC table correctly after a failover - Solution: Force former primary to shut down all its interfaces for one second when the failover happens (excluding heartbeat and reserved management interfaces):
#Config system ha
set link-failed-signal enable end
- This simulates a link failure that clears the related entries from MAC table of the switches.

NEW QUESTION 15
.....

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