NSE7_EFW-7.2 Q&As

Fortinet NSE 7 - Enterprise Firewall 7.2

Pass Fortinet NSE7_EFW-7.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/nse7_efw-7-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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.

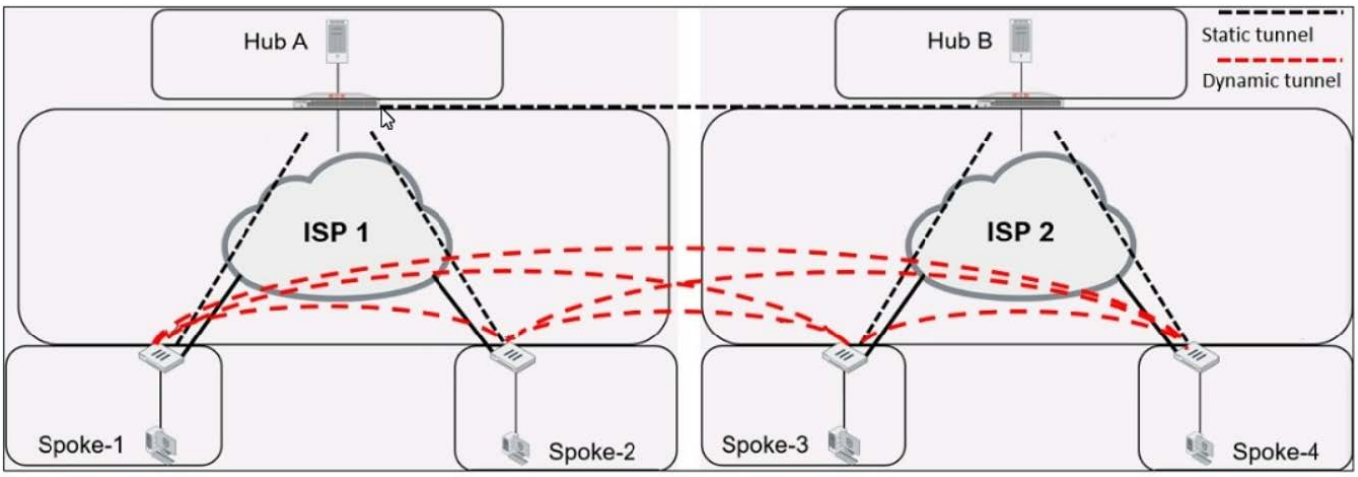
D. It detects only two-way failures.

Correct Answer: AC

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.

QUESTION 2

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

Correct Answer: AC

For the ADVPN feature to function properly on the hub, the following phase 1 parameters must be configured:

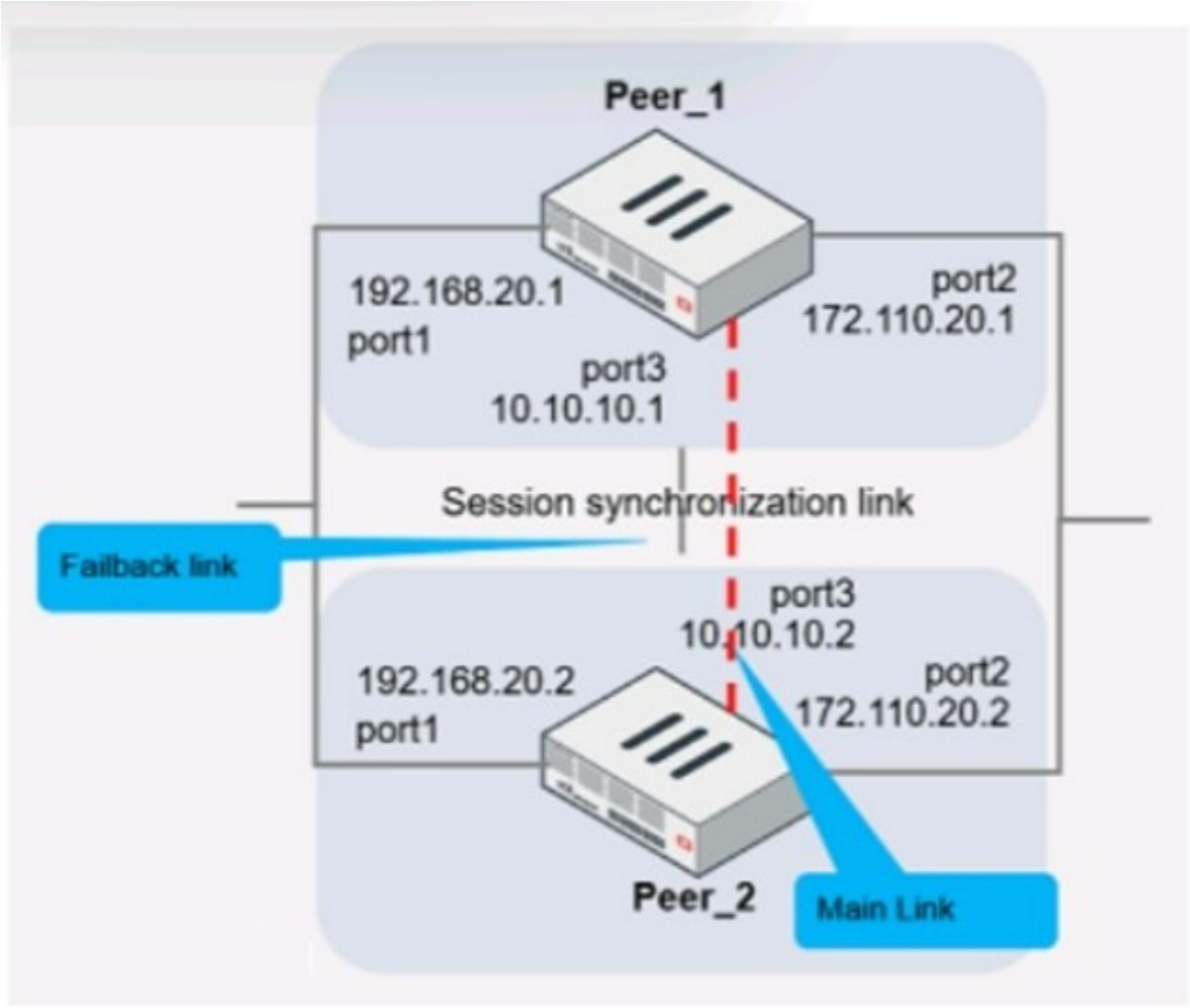
A. set auto-discovery-forwarder enable: This enables the hub to forward shortcut information to the spokes, which is essential for them to establish direct tunnels. C. set auto-discovery-receiver enable: This allows the hub to receive shortcut

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.

QUESTION 3

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 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

Correct Answer: D

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.

QUESTION 4

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

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

Correct Answer: BD

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 toestablish a secure tunnel, which is more efficient than IKE version 12. References: = IKE settings | FortiClient 7.2.2 - Fortinet Documentation, Technical Tip: How to configure IKE version 1 or 2 ... - Fortinet Community

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

Correct Answer: BC

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