

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.leads4pass.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

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 interfaces
- D. Set protected network to all

Correct Answer: A

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

QUESTION 3

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.

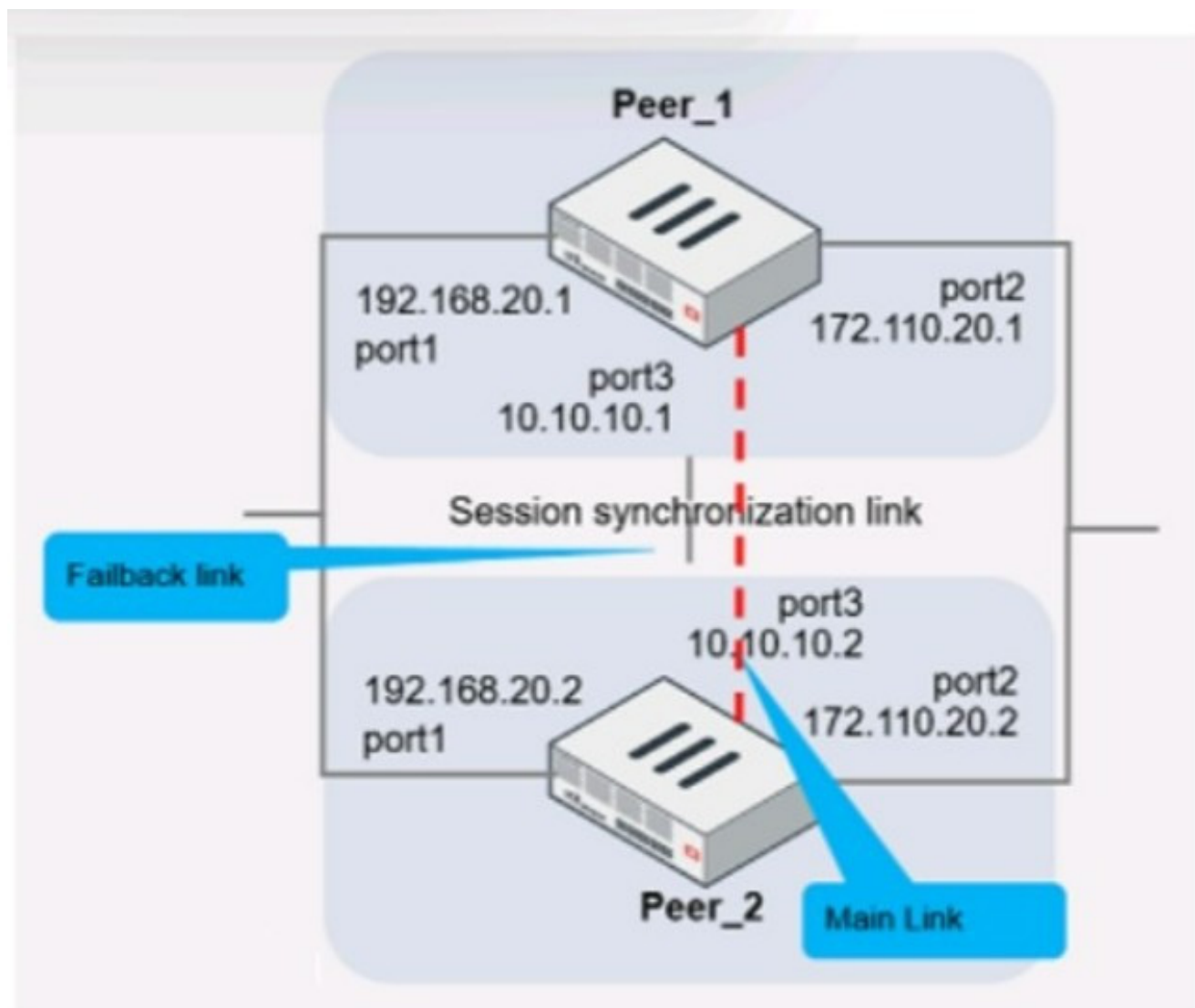
D. It exchanges a minimum of four messages to establish a secure tunnel

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 to establish a secure tunnel, which is more efficient than IKE version 1.2. References: = IKE settings | FortiClient 7.2.2 - Fortinet Documentation, Technical Tip: How to configure IKE version 1 or 2 ... - Fortinet Community

QUESTION 4

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 5

Which FortiGate in a Security Fabric sends logs 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

Correct Answer: B

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

policy. 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

QUESTION 6

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

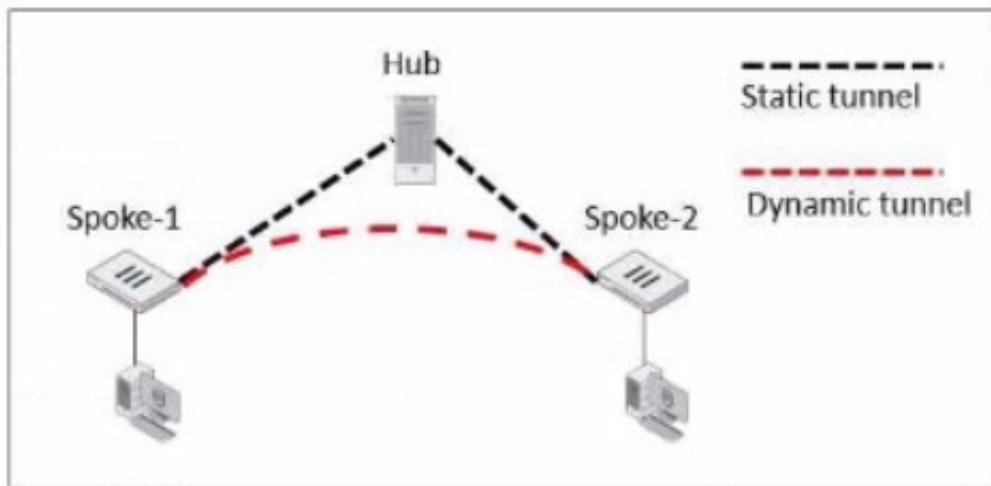
Correct Answer: B

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

QUESTION 7

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 does the hub send to Spoke-1 to bring up the dynamic tunnel?

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

Correct Answer: A

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.

QUESTION 8

Exhibit.

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

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

Refer to the exhibit, which contains the partial interface configuration of two FortiGate devices.

Which two conclusions can you draw from this configuration? (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

Correct Answer: AB

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). With `vrrp-virtual-mac enable`, 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).

QUESTION 9

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.

Correct Answer: AD

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.

QUESTION 10

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 configuration?

- 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 is disabled.
- D. The routing table shows a single IPsec virtual interface.

Correct Answer: C

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 disabled. 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.

QUESTION 11

In which two ways does FortiManager function when it is deployed as a local FDS? (Choose two)

- A. It can be configured as an update server, a rating server, or both.
- B. It provides VM license validation services.
- C. It supports rating requests from non-FortiGate devices.
- D. It caches available firmware updates for unmanaged devices.

Correct Answer: AB

When deployed as a local FortiGuard Distribution Server (FDS), FortiManager functions in several capacities. It can act as an update server, a rating server, or both, providing firmware updates and FortiGuard database updates.

Additionally, it plays a crucial role in VM license validation services, ensuring that the connected FortiGate devices are operating with valid licenses. However, it does not support rating requests from non-FortiGate devices nor cache firmware updates for unmanaged devices. Fortinet FortiOS Handbook: FortiManager as a Local FDS Configuration

QUESTION 12

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).

Correct Answer: BD

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.

QUESTION 13

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?

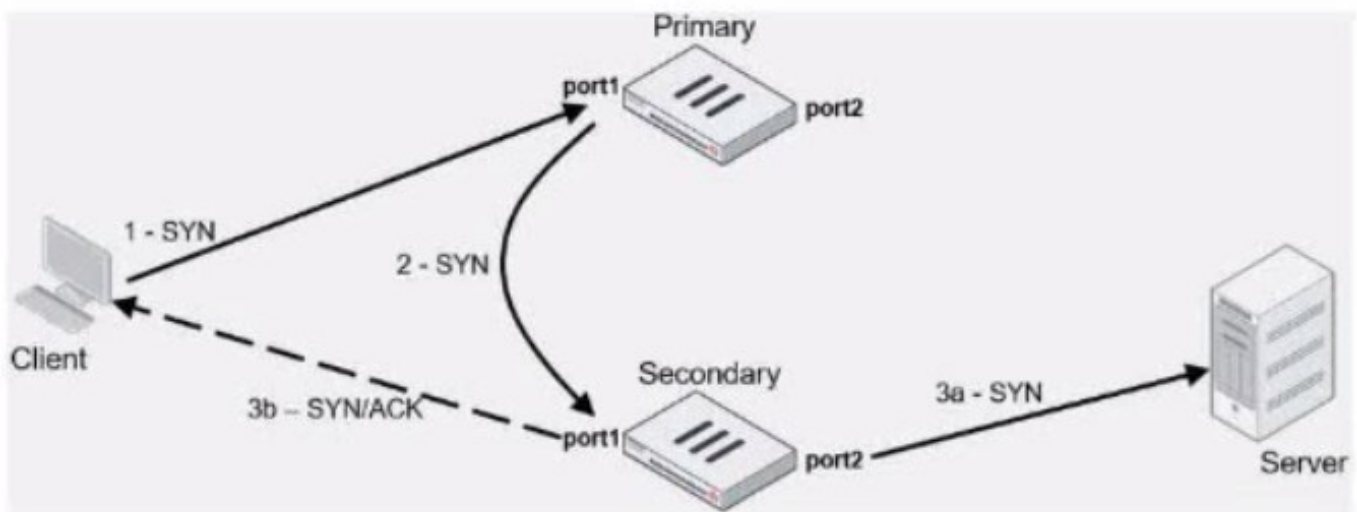
- A. NPs and CPs are enabled
- B. Only CPs are disabled
- C. Only NPs are disabled
- D. NPs and CPs are disabled

Correct Answer: D

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

QUESTION 14

Exhibit.



Refer to the exhibit, which contains an active-active load 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

Correct Answer: A

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.

QUESTION 15

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 server.fortiguard.net to the server list.
- B. Configure securewf.fortiguard.net on the default servers.
- C. Set update-server-location to automatic.

D. Configure server-type with the rating option.

Correct Answer: D

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.

[Latest NSE7_EFW-7.2 Dumps](#)

[NSE7_EFW-7.2 VCE Dumps](#)

[NSE7_EFW-7.2 Braindumps](#)