

Fortinet

Exam Questions NSE7_EFW-7.2

Fortinet NSE 7 - Enterprise Firewall 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).

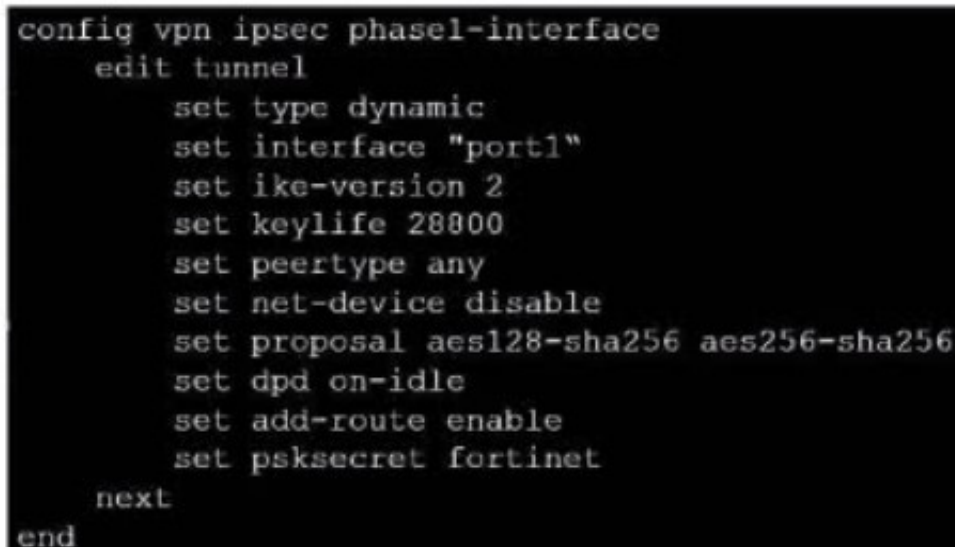
Answer: BD

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 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 3

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 configuration1?

- 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 s disabled.
- D. The routing table shows a single IPSec virtual interface.

Answer: C

Explanation:

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 disabled1. 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.

NEW QUESTION 4

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 vrdest 8.8.8.8	set vrdest 8.8.8.8
set vrdest-priority 30	set vrdest-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 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

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). With vrrp-virtual-mac enabled, 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 5

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 6

Which two statements about IKE version 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

Answer: BD

Explanation:

IKE version 2 supports the extensible authentication protocol (EAP), which allows for more flexible and secure authentication methods. IKE version 2 also exchanges a minimum of four messages to establish a secure tunnel, which is more efficient than IKE version 1. References: = IKE settings | FortiClient 7.2.2 - Fortinet

Documentation, Technical Tip: How to configure IKE version 1 or 2 ... - Fortinet Community

NEW QUESTION 7

After enabling IPS you receive feedback about traffic being dropped. What could be the reason?

- A. Np-accel-mode is set to enable
- B. Traffic-submit is set to disable
- C. IPS is configured to monitor

D. Fail-open is set to disable

Answer: D

Explanation:

Fail-open is a feature that allows traffic to pass through the IPS sensor without inspection when the sensor fails or is overloaded. If fail-open is set to disable, traffic will be dropped in such scenarios¹. References: = IPS | FortiGate / FortiOS 7.2.3 - Fortinet Documentation
When IPS (Intrusion Prevention System) is configured, if fail-open is set to disable, it means that if the IPS engine fails, traffic will not be allowed to pass through, which can result in traffic being dropped (D). This is in contrast to a fail-open setting, which would allow traffic to bypass the IPS engine if it is not operational.

NEW QUESTION 8

Which two statements about ADVPN are true? (Choose two.)

- A. You must disable add-route in the hub.
- B. All FortiGate 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 between spokes.

NEW QUESTION 9

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 10

Exhibit.

Script Name	Static Route
Comments	<div>0/255</div> <div>0/255</div>
Type	CLI Script
Run script on	Remote FortiGate Directly (...)
Script details	<pre># conf rout stat # edit 0 # set gateway 10.20.121.2 # set priority 20 # set device "wan1" # next # end</pre>

Refer to the exhibit, which contains a CLI script configuration on FortiManager. An administrator configured the CLI script on FortiManager but the script failed to apply any changes to the managed device after being executed.
What are two reasons why the script did not make any changes to the managed device? (Choose two)

- A. The commands that start with the # sign did not run.
- B. Incomplete commands can cause CLI scripts to fail.
- C. Static routes can be added using only TCI scripts.
- D. CLI scripts must start with #!.

Answer: AB

Explanation:

The commands that start with the # sign did not run because they are treated as comments in the CLI script. Incomplete commands can cause CLI scripts to fail because they are not recognized by the FortiGate device. The other options are incorrect because static routes can be added using CLI or GUI, and CLI scripts do not need to start with #!. References := Configuring custom scripts | FortiManager 7.2.0 - Fortinet Documentation, section "CLI script syntax".

NEW QUESTION 10

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 15

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-sender enabled to send shortcut advertisement messages to the spokes. Also, the hub would need to have auto-discovery-forwarder enabled 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. The ike-version does not need to be reconfigured on the hub if it's already set to version 2 and auto-discovery-receiver is not necessary on the hub because it's the one sending the advertisements, not receiving.

References:

? FortiOS Handbook - ADVPN

NEW QUESTION 18

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)