KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **NSE7_FSN_AR-7.6**

Title : Fortinet NSE 7 - Secure Networking 7.6 Architect

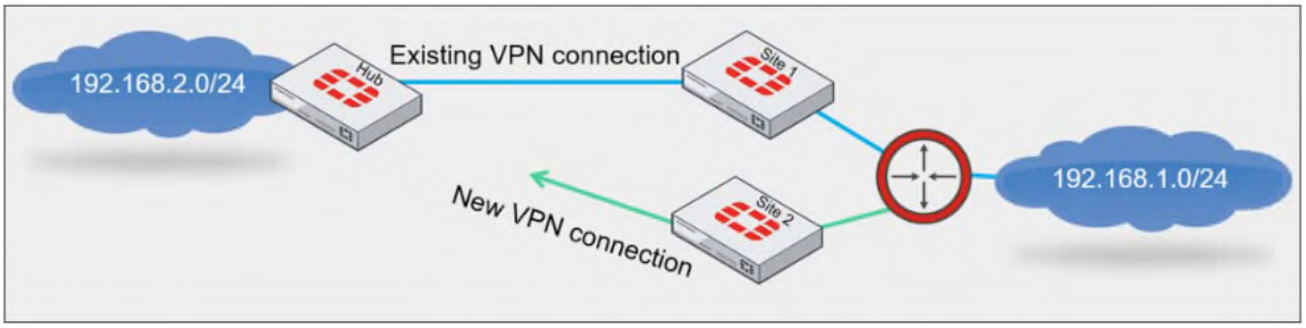
Version : DEMO

1.What is the diagnose test application ipsmonitor 5 command used for? (Choose one answer)
A. To disable the IPS engine
B. To provide information regarding IPS sessions
C. To restart all IPS engines and monitors
D. To enable IPS bypass mode
Answer: D
Explanation:
The correct answer is D.
The study guide shows the ipsmonitor test usage exactly:
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
5: Toggle bypass status
99: Restart all IPS engines and monitor
So diagnose test application ipsmonitor 5 is used to toggle bypass status, which corresponds to enabling IPS bypass mode.
Why the other options are wrong:
A is wrong because disabling the IPS engine is option 2, not 5.
B is wrong because the study guide does not define option 5 as IPS session information.
C is wrong because restarting all IPS engines and monitors is option 99, not 5.
So the verified answer is: D.

2.In which order does FortiGate consider the following elements during the route lookup process?
A. Policy routes, SD-WAN rules, Internet Service Database (ISDB) routes, BGP routes.
B. SD-WAN rules, ISDB routes, policy routes, BGP routes.
C. SD-WAN rules, policy routes, static routes, ISDB routes.
D. Policy routes, ISDB routes, SD-WAN rules, static routes.
Answer: D
Explanation:
FortiOS performs several routing checks before standard forwarding-table processing. The FortiOS 7.6 Administrator Study Guide describes the sequence explicitly. FortiGate first evaluates regular policy routes. If no applicable policy route forwards the packet, FortiGate evaluates Internet Service Database routes, followed by configured SD-WAN rules.
Only after those policy-routing mechanisms have been evaluated does FortiGate perform the standard forwarding information base (FIB) lookup. Static and dynamically learned routes, including BGP routes, are represented in this normal routing stage.
Consequently, among the available choices, the correct ordering is policy routes, ISDB routes, SD-WAN rules, and then static routes through the FIB.
Options A and B incorrectly place SD-WAN before ISDB or policy routing, while C incorrectly places SD-WAN ahead of the regular policy-routing stages. Therefore, D is correct.

3.Refer to the exhibit.

Network topology



The network diagram shows the addition of Site 2 with an overlapping network segment to the existing IPsec VPN connection between the hub and Site 1.

Which IPsec phase 2 configuration must you make on the FortiGate hub to enable equal-cost multipath (ECMP) routing when multiple remote sites connect with overlapping subnets?

A. Set route-overlap to either use-new or use-old.

B. Set multipath to enable.

C. Set route-overlap to allow.

D. Set net-device to ecmp.

Answer: C

Explanation:

Comprehensive and Detailed 100 to 150 words of Explanation From Secure Networking Architect Study Guides topics:

Fortinet documents three values for the phase 2 route-overlap setting: use-new, use-old, and allow. The required value for simultaneous VPNs advertising overlapping remote subnets is allow.

With route-overlap allow, FortiGate keeps the existing dial-up VPN active and also accepts the newly connected VPN. The Enterprise Firewall 7.6 Administrator Study Guide explicitly states that traffic from the central FortiGate is then load-balanced using equal-cost multipath across both VPNs. This directly satisfies the scenario and makes C correct.

The default use-new setting disconnects the existing VPN and accepts the new one, while use-old keeps the existing VPN and rejects the new connection. Neither produces ECMP. multipath enable and net-device ecmp are not the phase 2 commands FortiOS uses to permit overlapping dial-up VPN routes.

4.You want to configure two static routes: one that references a zone and a second one that references an SD-WAN member that belongs to that zone.

Which statement about this scenario is true? (Choose one answer.)

A. You cannot create static routes for individual SD-WAN members.

B. You cannot create static routes that reference an SD-WAN zone.

C. The destination subnets must be different.

D. The source subnets must be different.

Answer: C

Explanation:

FortiOS supports both route types described in the question. The FortiOS 7.6 Administrator Study Guide states that a static route can reference one or more SD-WAN zones and that FortiOS consequently installs an individual route for every member of the selected zone. It also states: “Alternatively, you can configure per-member static routes for more granular control over traffic.” Therefore, options A and B are

incorrect. Fortinet’s official configuration guidance likewise shows static routes referencing an SD-WAN zone.
The relevant duplicate-route restriction is based on the destination prefix. Fortinet courseware explains: “FortiOS doesn’t allow you to configure a static route for the same destination that references an interface.” Accordingly, a route referencing an SD-WAN zone and another route referencing one of that zone’s members cannot use identical destination subnets. They can use different or overlapping destination prefixes—for example, a less-specific route through the zone and a more-specific route through the individual member. The source subnets are not the required differentiator, eliminating option D.

5.Which exchange lakes care of DoS protection in IKEv2?
A. Create_CHILD_SA
B. IKE_Auth
C. IKE_Req_INIT
D. IKE_SA_NIT
Answer: C
Explanation:
The IKE_SA_INIT exchange in IKEv2 is responsible for DoS protection measures. During IKE_SA_INIT, before authentication and further exchange, the responder can use cookie challenges (per RFC 7296 and Fortinet VPN documentation). If a DoS attack is suspected (many requests from the same source), the responder replies with a cookie. Only after the initiator returns the correct cookie does the exchange proceed, protecting the responder from state exhaustion and certain forms of DoS traffic at the handshake stage.
References:
FortiOS VPN Manual: IKEv2 Exchange Process and DoS Protections
IKEv2 RFC 7296: Description of IKE_SA_INIT and DoS Cookie Mechanism