DUMPSARENA

Fortinet NSE 6Network Security 7.6 Support Engineer

Fortinet FCSS_NST_SE-7.6

Version Demo

Total Demo Questions: 2

Total Premium Questions: 23

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, FortiGate	23
Total	23

QUESTION NO: 1

A routing table contains a route for 192.0.2.0/24 through port3 with an administrative distance of 20 and a default route through port2 with an administrative distance of 10. Traffic destined for 192.0.2.10 is forwarded through port3. Why does FortiGate select port3?

A. The /24 route is the longest matching prefix.

B. The /24 route has a lower administrative distance.

C. The default route can be used only for unknown destinations.

D. The port3 route is selected because it has a higher administrative distance.

ANSWER: A

Explanation:

FortiGate selects routes by longest-prefix match before considering administrative distance. The 192.0.2.0/24 route is more specific than the default route and is therefore selected, even though its administrative distance is higher. Administrative distance is used when comparing routes with the same destination prefix length.

QUESTION NO: 2

An IPsec tunnel shows as established, but users report that protected traffic is not passing. A support engineer runs `diagnose vpn tunnel list` for the tunnel. Which two types of information can be verified directly from the output? (Choose two.)

A. The installed IPsec security associations for the tunnel.

B. The packet and byte counters for tunnel traffic.

C. The IPv4 firewall policy that accepted the traffic.

D. The complete IKE proposal negotiation exchange.

E. The FSSO group matched by the source user.

ANSWER: A B

Explanation:

The tunnel list output provides information about installed IPsec security associations, including the encryption and decryption SAs, and it shows traffic statistics such as packet and byte counters. These counters help determine whether FortiGate is encrypting outbound traffic or receiving and decrypting return traffic. The command does not replace IKE debug output for proposal negotiation or show firewall policy matching decisions.