DUMPSBOSS.

NSE7_SDW-6-4

Certification NSE7_SDW-6-4

Version Demo

Total Demo Questions: 3

Total Premium Questions: 35

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, SD-WAN configuration	6
Topic 2, SD-WAN rules and performance SLAs	12
Topic 3, SD-WAN deployment	9
Topic 4, SD-WAN troubleshooting	5
Topic 5, Mix Questions	3
Total	35

QUESTION NO: 1

Which statement correctly describes how BGP route tags are used with SD-WAN rules?

A. VPN topologies are formed using only BGP dynamic routing with SD-WAN.

B. Route tags are used for a BGP community and the SD-WAN rules are assigned the same tag.

C. BGP tags require that the adding of static routes be enabled on all ADVPN interfaces.

D. BGP tags match the SD-WAN rule based on the order that these rules were installed.

ANSWER: B

Explanation:

Route tags are used for a BGP community and the SD-WAN rules are assigned the same tag. In FortiOS, BGP communities can identify routes that share a particular routing characteristic or policy. A route map can match the relevant BGP community and set a route tag on the matching route. This numeric route tag is then available to SD-WAN rule matching, allowing the SD-WAN policy to select traffic associated with routes carrying that tag. For example, routes learned through BGP can be classified according to their community values, tagged through BGP route processing, and then handled by an SD-WAN rule configured with the corresponding route tag. This provides a direct link between dynamic-routing information and application-aware path selection: routing policy classifies the reachable prefixes, while SD-WAN policy applies the intended overlay-member preference and SLA behavior for traffic sent toward those prefixes. The tag must be consistently configured in the BGP route-policy processing and in the SD-WAN rule so that the rule can match the intended routes. Fortinet documents this integration as BGP route tagging for SD-WAN rules in the FortiOS New Features documentation; related configuration concepts are available in the FortiOS Administration Guide.

QUESTION NO: 2

Which statement correctly describes the relationship between SD-WAN and ADVPN in FortiOS?

A. Spoke support dynamic VPN as a static interface.

B. Dynamic VPN is not supported as an SD-WAN interface.

C. ADVPN interface can be a member of SD-WAN interface.

D. Hub FortiGate is limited to use ADVPN as SD-WAN member interface.

ANSWER: C

Explanation:

“ADVPN interface can be a member of SD-WAN interface.” is correct. In FortiOS, an ADVPN deployment uses IPsec tunnel interfaces to establish an overlay between hubs and spokes. Those tunnel interfaces can be added as SD-WAN members, allowing SD-WAN to apply its normal path-selection and performance-based steering capabilities to ADVPN connectivity. This integration lets a FortiGate use SLA health checks, link quality measurements, SD-WAN rules, and service-based routing decisions when selecting overlay paths. ADVPN further enhances the design by allowing eligible spokes to establish dynamic shortcut tunnels directly to one another, rather than always sending inter-spoke traffic through a hub. When ADVPN is used with SD-WAN, the dynamic overlay links participate in the broader SD-WAN design while preserving centralized policy and route control. This is particularly useful for scalable branch networks because it combines efficient spoke-to-spoke communication with SD-WAN’s automated selection of the best available path. Fortinet documents ADVPN as an SD-WAN-supported overlay use case in the FortiOS 6.4 Administration Guide; see also Fortinet’s SD-WAN new features documentation for SD-WAN and ADVPN capabilities.

QUESTION NO: 3

Which two benefits does FortiManager provide when organizing and managing a group of FortiGate devices? (Choose two.)

A. It simplifies the deployment and administration of SD-WAN on managed FortiGate devices.

B. It improves SD-WAN performance on the managed FortiGate devices.

C. It sends probe signals as health checks to the beacon servers on behalf of FortiGate.

D. It acts as a policy compliance entity to review all managed FortiGate devices.

E. It reduces WAN usage on FortiGate devices by acting as a local FortiGuard server.

ANSWER: A D

Explanation:

It simplifies the deployment and administration of SD-WAN on managed FortiGate devices. FortiManager provides centralized management for multiple FortiGate devices, allowing administrators to define, reuse, and install common configuration elements at scale. In an SD-WAN deployment, this centralization helps maintain consistent configurations across branches and reduces the operational effort involved in deploying or updating managed devices. FortiManager device groups, policy packages, scripts, and installation workflows are designed to make coordinated administration practical for large FortiGate estates.

It acts as a policy compliance entity to review all managed FortiGate devices. FortiManager includes policy and configuration-management capabilities that let administrators compare managed-device configurations with centrally defined policy packages and settings. This supports governance by identifying configuration differences, reviewing device status, and ensuring that intended security-policy changes are consistently installed across the managed FortiGate population. These functions provide centralized visibility and control, which are essential when maintaining standardized security and SD-WAN policy across many locations. See the FortiManager 6.4 Administration Guide and Fortinet's FortiManager product documentation for details on centralized device, policy, and configuration management.