Boost up Your Certification Score

Fortinet

NSE7_SSE_AR-26

Fortinet NSE 7 - FortiSASE 26 Architect

Exams Boost

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/nse7-sse-ar-26

Latest Version: 6.1

Question: 1

Refer to the exhibit.
Two hub-and-spoke groups are connected through redundant site-to-site IPsec VPNs between Hub 1 and Hub 2.
Which two configuration settings are required for spoke A1 to establish an auto-discovery VPN (ADVPN) shortcut with spoke B2? (Choose two.)

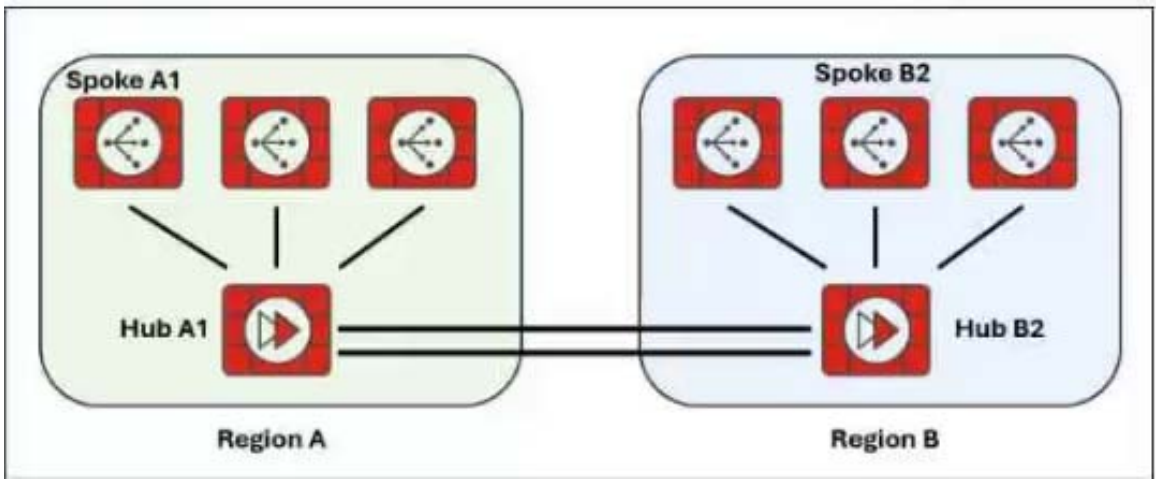


Exhibit — Hub-and-spoke ADVPN topology

A. On the spokes, auto-discovery-receiver must be enabled on the IPsec VPNs to the hub.
B. On the spokes, auto-discovery-sender must be enabled on the IPsec VPNs to hubs.
C. On the hubs, auto-discovery-receiver must be enabled on the IPsec VPNs to spokes.
D. On the hubs, auto-discovery-forwarder must be enabled on the IPsec VPNs to hubs.

Answer: A, D

Explanation:
ADVPN enables dynamic spoke-to-spoke IPsec shortcuts that eliminate unnecessary transit through hub devices after the initial discovery and negotiation process. In this scenario, spokes A1 and B2 belong to separate hub-and-spoke groups, interconnected through redundant IPsec tunnels.
Option A is correct because spoke devices use auto-discovery-receiver on their hub-facing IPsec Phase 1 interfaces. This enables the spokes to receive ADVPN shortcut discovery information needed to establish a direct tunnel to another spoke. Fortinet's ADVPN configuration examples explicitly demonstrate this receiver role.
Option D is correct because the interconnected hubs must forward the relevant ADVPN discovery messages across their inter-hub IPsec tunnels. Enabling auto-discovery-forwarder

allows discovery signaling to traverse the hub-to-hub connections so that spokes belonging to different regions can discover one another.
Option B reverses the standard spoke and hub discovery roles. The hub normally performs the sender role on its spoke-facing tunnels, whereas the spoke uses the receiver role.
Option C similarly assigns the receiver role to the wrong side of the hub-to-spoke relationship. The essential distinction is between receiving shortcut discovery at the spokes and forwarding discovery information between the hubs.
==========

Question: 2

Refer to the exhibit.
An SD-WAN zone configuration on the FortiGate GUI is shown.
What can you conclude about the zone and member configuration on this device?



Exhibit — FortiGate SD-WAN zones

A. The WAN2 zone contains no member.
B. You can delete any zone with the red icon.
C. You can delete only the WAN1 zone.
D. The HUB1 zone contains no member.

Answer: C

Explanation:
FortiGate SD-WAN zones are logical containers that group interfaces for traffic steering, route selection, and security-policy enforcement. The exhibit distinguishes zones from their underlying SD-WAN members through a hierarchical display.
Option C is correct. WAN1 is an empty, user-created zone and can be deleted because it has no SD-WAN member associations. The other zones must be evaluated according to their membership and whether they are system-defined.

WAN2 has an expansion indicator, showing that the zone contains member entries even though those entries are currently collapsed. Consequently, option A is incorrect: the absence of visible subordinate interfaces does not prove that a zone has no members.
HUB1 also has an expansion indicator. Its members are hidden by the collapsed view, so option D is incorrect.
The red icon is not a universal deletion indicator. In particular, the built-in virtual-wan-link zone must not be treated as an ordinary removable custom zone. An administrator must distinguish interface or zone operational status from configuration eligibility for deletion.
Before removing a custom zone, its members and any references in firewall policies or SD-WAN rules must be examined.
==========

Question: 3

You are configuring SD-WAN to load balance network traffic and you want to take into account the link quality.
Which two facts should you consider? (Choose two.)

A. When applicable, FortiGate load balances the traffic through all members that meet the SLA target.
B. You can select the lowest cost service level agreement (SLA) strategy and allow SD-WAN load balancing.
C. You can select the best quality strategy and allow SD-WAN load balancing.
D. The best quality strategy is compatible with the session, spillover, and volume load balance algorithms.

Answer: A, B

Explanation:
FortiGate SD-WAN can distribute traffic over multiple WAN links while applying performance-based eligibility checks. These checks measure network conditions such as latency, jitter, and packet loss against defined service-level agreement thresholds.
Option A is correct because FortiGate can load balance sessions across available SD-WAN members that satisfy the configured SLA target. An interface that fails the required performance criteria is excluded from the eligible load-balancing set under normal SLA-compliant operation.
Option B is correct because current FortiOS versions support load balancing within the Lowest Cost (SLA) strategy. The configuration uses set mode sla together with set load-balance enable under the relevant SD-WAN service rule. Importantly, the load-balancing algorithm does not use interface cost to select individual links once SLA-based load balancing is enabled.
Option C is incorrect because Best Quality is a separate strategy that selects preferred members based on measured link-quality metrics. It is not the supported SLA-based multi-link load-balancing configuration described in the question.
Option D is incorrect because the legacy session, spillover, and volume terminology does not describe supported Best Quality load-balancing algorithms in this context.

FortiOS 7.4.1 and later integrated the former Maximize Bandwidth strategy into the current load-balancing configuration model.
==========

Question: 4

What are three key routing principles of SD-WAN? (Choose three.)

A. SD-WAN members are skipped if they do not have a valid route to the destination.
B. Internet Service Database (ISDB) routes have precedence over SD-WAN rules.
C. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.
D. SD-WAN rules are skipped if the best route to the destination is a static route.
E. Routes to directly connected subnets have precedence over SD-WAN rules.

Answer: A, C, E

Explanation:
FortiGate SD-WAN integrates policy-based traffic steering with the traditional routing subsystem. SD-WAN rules do not automatically override routing-table decisions; they operate within the route-selection framework.
Option A is correct. A member selected by an SD-WAN rule must have a valid route toward the destination. If the selected member cannot reach the destination, FortiGate excludes that member and evaluates another eligible candidate.
Option C is correct. Under default SD-WAN routing behavior, the best route to the destination must point toward an SD-WAN member before SD-WAN service-rule evaluation applies. If the best route points to a non-SD-WAN interface, conventional routing handles the traffic instead.
Option E is correct because a directly connected route can take precedence when it is the best matching route. FortiGate does not unnecessarily divert locally reachable destinations into SD-WAN processing.
Option B is incorrect because the Internet Service Database supplies application and destination classification information; it does not establish a universal routing-precedence rule above SD-WAN.
Option D is incorrect because a static route does not inherently bypass SD-WAN. Static routes commonly provide reachability through SD-WAN member interfaces.
The fundamental principles are route eligibility, valid member reachability, and preservation of conventional routing decisions outside the SD-WAN domain.
==========

Question: 5

An organization is integrating a cloud-delivered security operations capability with its secure access service edge (SASE) architecture to enhance threat detection, investigation, and response

across a distributed environment of users and endpoints. The security team is particularly focused on improving real-time threat monitoring and gaining unified visibility into security events across the infrastructure.
Which two benefits are achieved by integrating SOC-as-a-Service (SOCaaS) with FortiSASE? (Choose two.)

A. Provides bandwidth usage analytics
B. Continuous threat monitoring across all connected endpoints
C. Eliminates the need for endpoint protection software
D. Centralized visibility into all threat events

Answer: B, D

Explanation:
FortiGuard SOC-as-a-Service provides managed security monitoring, threat investigation, alert triage, and incident-response assistance for organizations that require dedicated security operations capabilities.
Option B is correct because SOCaaS provides continuous monitoring of security telemetry forwarded from protected FortiSASE and FortiGate environments. Fortinet's managed security specialists investigate suspicious activity, correlate events, and escalate validated incidents. This capability provides ongoing visibility into security threats affecting connected users and protected endpoints, within the scope of integrated telemetry sources.
Option D is correct because SOCaaS centralizes security event analysis and incident visibility. Logs and alerts collected from different enforcement points can be correlated to support investigations and coordinated remediation, reducing the operational fragmentation associated with independent monitoring systems.
Option A is incorrect because bandwidth analytics primarily belongs to network monitoring, traffic analytics, and digital experience monitoring rather than the core SOCaaS security-operations function.
Option C is incorrect because SOCaaS does not replace endpoint protection. FortiClient, endpoint detection and response, and other security controls continue to provide essential prevention and endpoint telemetry.
The Study Guide describes SOCaaS as a 24/7 managed service incorporating FortiGuard intelligence, expert investigation, and security orchestration capabilities.
==========

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer

