Boost up Your Certification Score

Fortinet

NSE5_SDW_AD-7.6

Fortinet NSE 5 - SD-WAN 7.6 Core Administrator



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/nse5-sdw-ad-7-6

Latest Version: 6.0

Question: 1

A branch requires local internet access through two ISP circuits. It has no requirement to reach another site or send internet traffic through a hub.
Branch LAN -- FortiGate -- wan1 -- ISP-A -- Internet
\-- wan2 -- ISP-B -- Internet
Which description of this SD-WAN design is correct?

A. The ISP circuits are overlays, and a separate VPN underlay is required.
B. The ISP circuits are underlays, and a site-to-site VPN overlay is not required for this local internet requirement.
C. The ISP circuits are underlays, and a site-to-site VPN overlay is required whenever two members are configured.
D. The ISP circuits are overlays, and they can replace the branch underlay connections.

Answer: B

Explanation:
The two ISP circuits provide the transport connectivity, so they belong to the underlay. A VPN overlay provides logical connectivity across sites when such connectivity is required. This branch only needs direct internet access (DIA), so configuring two SD-WAN members does not itself require a site-to-site VPN or a hub.

Question: 2

In FortiOS 7.6.3, wan1 and wan2 are SD-WAN members in the zone Internet. A firewall policy from LAN must allow traffic to use either member. The SD-WAN rules will choose the member for matching traffic. Which outgoing interface should the administrator select in the firewall policy?

A. Both member interfaces, wan1 and wan2, directly.
B. wan1, with wan2 listed only in the policy comment.
C. A new non-SD-WAN zone containing the same interfaces.
D. The Internet SD-WAN zone.

Answer: D

Explanation:
Select the Internet SD-WAN zone as the outgoing policy interface. In FortiOS 7.6.3, firewall policies reference SD-WAN zones rather than individual member interfaces. Allowing the zone and selecting a particular member are separate decisions: the policy permits traffic through the zone, while the applicable SD-WAN rule performs member selection.

Question: 3

An administrator has selected passive mode for an SD-WAN performance SLA. Real TCP application traffic is available, but the matching firewall policy has not yet been prepared for passive WAN health measurement.
Which two policy settings are required to collect passive measurements for that traffic in FortiOS 7.6.3? (Choose two)

A. Enable passive-wan-health-measurement on the policy that accepts the traffic.
B. Use an individual SD-WAN member as the policy outgoing interface instead of its zone.
C. Set the policy outgoing interface to the appropriate SD-WAN zone.
D. Keep auto-asic-offload enabled on that policy as a prerequisite for passive measurement.
E. Replace passive mode with active mode before the policy can contribute measurements.

Answer: A, C

Explanation:
Passive health measurement analyzes real TCP session information. The accepting firewall policy must enable passive-wan-health-measurement, and its outgoing interface must be an SD-WAN zone.

Question: 4

An active SD-WAN health check is receiving probe replies, and its diagnostic state is alive. A single SLA target has a latency threshold of 50 ms. The measured latency is 85 ms, while all other metrics satisfy that target.
Which conclusion is supported by this information alone?

A. The member is reachable, but it does not satisfy the SLA target; the actual traffic path requires additional rule and routing information.
B. The member is dead rather than merely out of SLA, because exceeding the latency threshold overrides the reported alive state.
C. The member remains alive and meets the SLA target, because receiving probe replies takes precedence over the configured latency threshold.
D. Every matching application must stop using the member, because an SLA target violation has the same effect as an unreachable link.

Answer: A

Explanation:
The member is alive, but 85 ms exceeds the target limit of 50 ms. Reachability therefore does not imply that the SLA target is met. The supplied information does not identify the matching SD-WAN rule, its strategy or fallback conditions, or the available routes, so it cannot establish the final traffic path.

Question: 5

A matching SD-WAN rule on FortiOS 7.6.3 has the following settings:
set mode manual
set priority-members 2 1
set load-balance disable
Member 2 is wan2, and member 1 is wan1. Both members are available and have valid routes to the destination. Measured latency is 70 ms on wan2 and 15 ms on wan1. No failover or recovery transition is in progress.
Which member should this rule prefer for a new matching session?

A. wan1, because its measured latency is lower.
B. Both members, because they are alive.
C. wan2, because it is first in priority-members.
D. wan1, because member ID 1 takes precedence over member ID 2.

Answer: C

Explanation:
Manual strategy uses the configured member preference order. The list places member 2 (wan2) first. Both candidates are usable, load balancing is disabled, and no recovery transition is in progress, so the rule prefers wan2.

Question: 6

A Best Quality SD-WAN rule uses latency as its quality factor. Both candidates have valid routes and the same measured latency of 220 ms.
The relevant settings are:
set mode priority
set priority-members 2 1
set link-cost-factor latency
set link-cost-threshold 10
Member 2 is wan2; member 1 is wan1.
Which interpretation of the configured preference is correct?

A. wan1 receives the preference because it has the lower member ID; the measured latency is unchanged.
B. wan2 receives the preference in the metric comparison; its measured latency is not physically reduced.
C. wan2 receives the preference by reducing its actual measured latency from 220 ms to 200 ms.
D. wan1 receives the preference by reducing its actual measured latency from 220 ms to 200 ms.

Answer: B

Explanation:
Member 2 (wan2) is first in priority-members, so it receives the configured comparison preference. The documented latency example applies the advantage as latency /(1 + threshold). With equal 220 ms

measurements and a 10% threshold, wan2 has a comparison value of 220 /1.10 = 200 ms, versus 220 ms for wan1. This affects selection; it does not improve the actual 220 ms latency.

Question: 7

A Lowest Cost (SLA) rule matches a new session. Load balancing is disabled, minimum-sla-meet-members is 1, and priority-members is 3 2 1. All three members are alive and have usable routes. The rule uses one SLA target, and all other rule and zone settings use their defaults.

Member	Interface	Cost	Meets the rule's SLA target
1	wan1	5	No
2	wan2	20	Yes
3	wan3	20	Yes

Which interface should the rule select?

A. wan1
B. wan2
C. Both wan2 and wan3
D. wan3

Answer: D

Explanation:
Members 2 and 3 both meet the SLA target, satisfying the minimum count of one qualifying member. Their costs are equal, and load balancing is disabled. The tie is resolved by priority-members, which places member 3 first, so the selected interface is wan3.

Question: 8

A Lowest Cost (SLA) rule uses load-balance enable and hash-mode source-ip-based. All listed members are configured in the rule and have usable routes.
There are no additional eligibility restrictions.

Interface	Cost	Meets the required SLA target
wan1	5	Yes
wan2	30	Yes
wan3	1	No

Which two statements describe this rule while these conditions remain unchanged? (Choose two)

A. wan1 and wan2 are in the eligible load-balancing pool despite their different costs.
B. wan2 is excluded because its cost is higher than wan1.
C. wan3 joins the pool because it has the lowest cost.

D. The source-ip-based method keeps traffic from a given source IP on the same selected interface under the stated unchanged conditions.
E. The rule must be changed to Manual mode before load balancing can be used.

Answer: A, D

Explanation:
With load balancing enabled inside an SLA rule, all usable configured members that meet the target can participate. Both wan1 and wan2 therefore belong to the eligible pool despite their different costs. The source-ip-based hash method sends traffic from a given source IP through the same selected interface while the stated candidate conditions remain unchanged.

Question: 9

An administrator is troubleshooting ordinary IPv4 policy-based routes on FortiOS 7.6.3. The packet matches the policy-route address, protocol and port criteria.
Which three statements about completing the forwarding decision are correct? (Choose three)

A. If only an outgoing interface is configured, FortiGate looks for a gateway using the routing table filtered by that interface.
B. If both outgoing interface and gateway are configured, no routing-table reachability check is needed.
C. If only a gateway is configured, FortiGate looks for an outgoing interface using the routing table filtered by that gateway.
D. If the required forwarding information cannot be resolved, FortiGate can continue to the next policy route.
E. Matching the address and port criteria guarantees that the current policy route is used.

Answer: A, C, D

Explanation:
A policy route must provide enough information to forward the packet. An interface-only rule needs gateway resolution filtered by that interface, and a gateway-only rule needs interface resolution filtered by that gateway. If the required forwarding information cannot be found, that policy route does not match and FortiGate continues evaluating the list; ordinary routing is used if no policy route matches.

Question: 10

An established source-NAT (SNAT) session on FortiOS 7.6.3 uses wan1. The global snat-route-change setting is disabled. A routing change makes a route through wan2 preferable, but the original route through wan1 remains active and usable. No other session-clearing or failure event occurs.
What is the documented default behavior for this existing SNAT session after that routing change?

A. It immediately moves to wan2 while retaining its old SNAT selection.
B. It must be deleted because an active session cannot survive a route preference change.
C. It keeps using wan1 while the original route remains active.
D. It immediately moves to wan2 and applies a new SNAT selection.

Answer: C

Explanation:
With SNAT enabled, an existing session normally keeps its outbound interface after a routing change as long as its old route remains active. Therefore this session keeps wan1 under the supplied conditions.

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

