



Fortinet NSE7_SSE_AR-26 Dumps

Shared by Osborne on 12-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

An administrator is attempting to create two static routes: one for the SD-WAN zone wan-link and one pointing to a specific SD-WAN member interface that currently belongs to the wan-link zone.

Which configuration is required to make this scenario valid? (Choose one answer.)

Options:

- A- The destination subnets of the two static routes must be different.
- B- Both routes must have the same administrative distance to allow equal-cost multipath (ECMP).
- C- The destination subnet configured on the SD-WAN zone cannot be a default route.
- D- SD-WAN member must be an IPsec interface.

Answer:

A

Explanation:

According to the Fortinet SD-WAN 7.6 Core Administrator Study Guide, Routing and Sessions, page 193, FortiOS supports static routes referencing SD-WAN zones and individual member interfaces. However, duplicate destination routes cannot simultaneously reference a zone and one of its individual member interfaces.

Option A is correct: FortiOS requires the two static routes to have different destination prefixes. When a static route references an SD-WAN zone, FortiGate creates forwarding entries for the members belonging to that zone. Configuring an additional route with the identical destination prefix through an individual member creates a conflicting route definition.

Overlapping destination networks are permitted when their prefixes differ. For example, a zone-based route could reference 10.0.0.0/8, while a member-specific route references 10.2.0.0/16.

Option B is incorrect: Equal administrative distance does not resolve the duplicate-route restriction. ECMP is not a substitute for valid route configuration.

Option C is incorrect: FortiOS supports default static routes (0.0.0.0/0) referencing SD-WAN zones.

Option D is incorrect: SD-WAN members can include physical interfaces, VLAN interfaces, IPsec tunnels, and other supported interface types.

Therefore, the two static routes must have different destination prefixes, although overlapping

networks are allowed.

Exact Source Reference:

Fortinet SD-WAN 7.6 Core Administrator Study Guide, pages 192--193 --- Routing and Sessions.

FortiOS 7.6 Administration Guide --- Adding a Static Route and SD-WAN Members and Zones.

Question 2

Question Type: MultipleChoice

What is the benefit of branch on-ramp deployment with FortiSASE? (Choose one answer.)

Options:

- A- To secure internet traffic for small remote offices.
- B- To provide access to private applications using the bookmark portal.
- C- To manage branch location endpoints.
- D- To provide device compliance checks using zero trust network access (ZTNA) tags.

Answer:

A

Explanation:

According to the FortiSASE 25 Enterprise Administrator Study Guide, page 25, branch on-ramp deployment enables organizations to secure outbound internet traffic from branch locations by connecting their existing network infrastructure to FortiSASE.

Option A is correct: Branch on-ramp allows remote offices and branch locations to establish secure IPsec VPN tunnels between their FortiGate or supported third-party network devices and FortiSASE points of presence (PoPs). Traffic is forwarded through these tunnels, allowing FortiSASE to deliver cloud-based security inspection and enforcement.

The study guide explains that connected branches can benefit from Secure Internet Access (SIA), Secure SaaS Access (SSA), and Secure Private Access (SPA).

Option B is incorrect: Although branch on-ramp supports secure private application access, providing access through a bookmark portal is not its primary deployment benefit.

Option C is incorrect: Branch on-ramp provides secure network connectivity and traffic

inspection. It is not designed primarily for endpoint inventory, administration, or lifecycle management.

Option D is incorrect: The study guide explicitly states that FortiClient installation is not required for branch edge-device deployments and that ZTNA tags are not supported in this configuration.

Therefore, branch on-ramp primarily enables organizations to extend FortiSASE cloud security services to branch offices and secure their internet-bound traffic.

Exact Source Reference:

FortiSASE 25 Enterprise Administrator Study Guide, page 25 --- Thick Edge Use Case, including secure branch outbound traffic and branch on-ramp.

FortiSASE 25 Enterprise Administrator Study Guide, page 26 --- FortiSASE Branch On-Ramp Configuration.

FortiSASE 25 Enterprise Administrator Study Guide, page 27 --- Edge-Device Policies, explaining the lack of ZTNA tag support.

Question 3

Question Type: MultipleChoice

An administrator is enforcing endpoint network lockdown using FortiSASE to ensure that devices access the internet only under defined security conditions. The lockdown state must be released automatically when the endpoint meets specific trust or connectivity criteria.

Which two conditions can trigger the release of the network lockdown on an endpoint? (Choose two answers.)

Options:

- A- The endpoint is detected as being on-net.
- B- The endpoint establishes a connection to the FortiSASE tunnel.
- C- The endpoint is rebooted.
- D- The endpoint is evaluated as compliant using security posture tags.

Answer:

A, B

Explanation:

According to the FortiSASE 25 Enterprise Administrator Study Guide, page 88, FortiClient automatically exits network lockdown when the endpoint is detected as on-net or successfully establishes a FortiSASE tunnel.

Option A is correct: FortiSASE uses on-net detection rules to identify whether an endpoint is connected to a trusted corporate network. When the endpoint satisfies the configured on-net rules, FortiClient can release network lockdown because internet traffic can be protected by the organization's on-premises security infrastructure, such as FortiGate.

Option B is correct: Network lockdown prevents unrestricted LAN and internet access when an off-net endpoint fails to establish its required FortiSASE tunnel within the configured grace period. Once the tunnel is successfully established, FortiClient releases the lockdown, allowing internet traffic to be secured through FortiSASE.

Option C is incorrect: Rebooting the endpoint does not independently satisfy either release condition. FortiClient continues enforcing the configured security requirements.

Option D is incorrect: Security posture tags evaluate endpoint compliance and support conditional access policies. However, posture compliance alone is not identified as a network-lockdown release condition.

The two documented release conditions are on-net detection and successful FortiSASE tunnel establishment.

Exact Source Reference:

FortiSASE 25 Enterprise Administrator Study Guide, page 86 --- On-Net Rule Sets.

FortiSASE 25 Enterprise Administrator Study Guide, page 88 --- On-Net and Off-Net Features--- Network Lockdown.

FortiSASE-Sovereign 26.2.a Administration Guide, page 67 --- On/Off-Net Settings.

Question 4

Question Type: MultipleChoice

In which order does FortiGate consider the following elements during the route lookup process? Choose one answer.

Options:

- A- SD-WAN rules, ISDB routes, policy routes, BGP routes
- B- Policy routes, SD-WAN rules, Internet Service Database (ISDB) 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:

In FortiOS (including FortiOS 7.6), FortiGate follows a strict and well-defined route lookup order when determining how to forward traffic. This order is critical for understanding SD-WAN behavior and is explicitly referenced in the FCSS SD-WAN curriculum. The correct lookup sequence is: Among the options provided, only Option D correctly reflects the beginning of this sequence by placing policy routes first, followed by ISDB routes, then SD-WAN rules, and finally static routes (representing the routing table). Therefore, the correct answer is D. An operational review should distinguish the rule that matches the traffic from the interface that is ultimately selected. Valid forwarding also depends on destination route eligibility, current member state and the applicable SLA or quality-selection algorithm. A diagnostic showing configured members alone is not conclusive evidence that all those members will carry a particular flow. When troubleshooting, correlate the configured SD-WAN service with `diagnose sys sdwan service4`, the live session entry and the routing table. An application signature, an IP route and a health-check result describe different decision stages; treating them as interchangeable can produce incorrect conclusions about the egress interface.

Question 5

Question Type: MultipleChoice

You plan a large SD-WAN deployment for a global company. You want to divide the network architecture into five geographical regions and install two hubs in each region for increased redundancy. You expect a significant amount of traffic within each region and limited traffic flow between spokes in different regions. You plan to connect the small branch sites to only the closest hub in their regions and the large branch sites to the two hubs in the regions. Which statement about your plan is true? Choose one answer.

Options:

- A- It is possible. You should use eBGP as the routing protocol between the regions.
- B- It is not possible. FortiOS 7.6 supports multihub topologies with up to four hubs.

- C- It is possible. You should use FortiManager and the overlay orchestrator multihub topology to simplify the deployment.
- D- It is not possible. In a region, all spokes must have either single-hub or dual-hub connectivity.

Answer:

A

Explanation:

The described design is a multi-region SD-WAN architecture, where: According to Fortinet's SD-WAN Architecture for Enterprise guidance, when deploying multiple ADVPN regions, eBGP is the recommended routing protocol between regions. Each region operates as an independent routing domain (typically iBGP within the region), while eBGP is used to exchange routes between regional hubs. This approach: This is explicitly documented in Fortinet guidance for "Using eBGP between regions with intra-region ADVPN", which confirms that the architecture described in the question is valid and recommended when eBGP is used between regions. Why the other options are incorrect: Therefore, the correct and documented conclusion is that the plan is possible and eBGP should be used as the routing protocol between regions, which corresponds to Answer A. A deployment should preserve the distinction between the physical or logical WAN underlay, the IPsec overlay and the SD-WAN zone that groups forwarding members. These layers can have different routing and security-policy requirements. The configured architecture must also allow the required traffic paths and failover behavior rather than assuming every available interface is interchangeable.

=====

Question 6

Question Type: MultipleChoice

Refer to the exhibits. Two SD-WAN event logs, the member status, the SD-WAN rule configuration, and the health-check configuration for a FortiGate device are shown. Immediately after the log messages are displayed, how will the FortiGate steer the traffic based on the information shown in the exhibits? Choose one answer.

SD-WAN event logs

Identity	
Device ID	FGVM02TM25002088
Device Name	branch1_fgt
Type	
Sub Type	sdwan
Type	event
Alerts	
Action	
Level	notice
General	
Log Description	SDWAN status
Log ID	0113022923
Member	1
Message	Member status changed. Member out-of-sla.
Virtual Domain	root
Others	
Date	2025-07-01
Date/Time	2025-07-01 05:00:25
Destination End User ID	3
Destination Endpoint ID	3
Destination Geo ID	0
Device Time	2025-07-01 05:00:25
Device Time Zone	-0700
Event Time	2025-07-01 05:00:25
Event Type	Health Check
Health Check	Corp_HC
Log Flag	0
New Value	1
Old Value	2
SLA Target ID	1
Source City	Sunnyvale

SD-WAN rule configuration

```
branch1_fgt (service) # show
config service
edit 1
set name "Critical-DIA"
set mode sla
set src "LAN-net"
set internet-service enable
set internet-service-app-ctrl 16920 41469
set internet-service-app-ctrl-category 28
config sla
edit "Corp_HC"
set id 1
next
end
set priority-members 1 2
next
```

SD-WAN health-check configuration

```
branch1_fgt (health-check) # show
config health-check
edit "Corp_HC"
set server "198.18.1.1" "198.18.1.2"
set member 1 2
config sla
edit 1
set latency-threshold 150
set jitter-threshold 50
set packetloss-threshold 5
next
end
end
```

SD-WAN member status

```
branch1_fgt # diagnose sys sdwan member
Member(1): type: 0, transport-group: 0, interface: port1, flags=0x0,
gateway: 192.2.0.2, source 192.2.0.1, priority: 1 1024, weight: 0
Member(2): type: 0, transport-group: 0, interface: port2, flags=0x0,
gateway: 192.2.0.10, source 192.2.0.9, priority: 1 1024, weight: 0
Member(3): type: 0, transport-group: 0, interface: port4, flags=0x0,
source 172.16.0.1, priority: 1 1024, weight: 0
```

Exhibit 1

Options:

- A- FortiGate skips SD-WAN rule ID 1.
- B- FortiGate uses port2 to steer the traffic for SD-WAN rule ID 1.
- C- FortiGate uses port1 to steer the traffic for SD-WAN rule ID 1.
- D- FortiGate uses port1 or port2 to steer the traffic for SD-WAN rule ID 1.

Answer:**B**

Explanation:

The SD-WAN event log shows member 1 transitioning out of SLA. The member diagnostics identify member 1 as port1 and member 2 as port2. The service's priority list places port1 before port2, so a properly eligible port2 would be the next forwarding choice when port1 no longer meets the required threshold. This makes option B the intended answer. However, the screenshots do not independently establish port2's current SLA pass state and the complete effective service selection conditions at the instant of the event. A single member's out-of-SLA log is insufficient to prove that port2 is healthy, reachable for the destination and selected immediately after the event. Option A is not a universal consequence of one SLA failure; option C incorrectly assumes port1 remains eligible; option D is not proven either because the configuration is not shown to be in a multi-member load-balancing state. To verify B, inspect 'diagnose sys sdwan service4 1' and the health-check status after the event, confirming member 2 is selected and destination-route eligible. The item is conditionally supported, not fully established by the current exhibit alone.

Verification qualification: Port2 must be shown operational and in SLA; the exhibit alone does not prove that state. Reference:

<https://docs.fortinet.com/document/fortigate/7.6.0/cli-reference/838040159/config-system-sdwan>

=====



To Get Premium Files for NSE7_SSE_AR-26
Visit

https://www.p2pexams.com/products/nse7_sse_ar-26

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/nse7-sse-ar-26>

20%
DISCOUNT

P2P
exams