Fortinet NSE5_SSE_AD-7.6 NSE 5 Practice Questions

Shared by Armstrong on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibits.

Routing Table on FortiGate

```
branch1_fgt # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 192.2.0.2, port2, [1/0]
```

The administrator increases the member priority on port2 to 20. Upon configuration changes and the receipt of new packets, which two actions does FortiGate perform on existing sessions established over port2? (Choose two.)

Options:

A- FortiGate updates the gateway information of the sessions with SNAT so that they use port1 instead of port2.
B- FortiGate flags the SNAT session as dirty only if the administrator has assigned an IP pool to the firewall policies with NAT.
C- FortiGate routes only new sessions over port1.
D- FortiGate continues routing all existing sessions over port2.
E- FortiGate flags the sessions as dirty.

Answer:

A, E

Question 2

Question Type: MultipleChoice

Which three FortiSASE use cases are possible? (Select three answers)

Options:

A- Secure Internet Access (SIA)

B- Secure SaaS Access (SSA)
C- Secure Private Access (SPA)
D- Secure VPN Access (SVA)
E- Secure Browser Access (SBA)

Answer:

A, B, C

Explanation:

According to the FortiSASE 7.6 Architecture Guide and the FCP - FortiSASE 24/25 Administrator study materials, the FortiSASE solution is structured around three primary pillars or 'use cases' that address the security requirements of a modern distributed workforce.

Secure Internet Access (SIA) (Option A): This use case focus on protecting remote users as they browse the public internet. It utilizes a full cloud-delivered security stack including Web Filtering, DNS Filtering, Anti-Malware, and Intrusion Prevention (IPS) to ensure that users are protected from web-based threats regardless of their physical location.

Secure SaaS Access (SSA) (Option B): This use case addresses the security of cloud-based applications (like Microsoft 365, Salesforce, and Dropbox). It leverages Inline-CASB (Cloud Access Security Broker) to identify and control 'Shadow IT'---unauthorized cloud applications used by employees---and applies Data Loss Prevention (DLP) to prevent sensitive information from being leaked into unsanctioned SaaS platforms.

Secure Private Access (SPA) (Option C): This use case provides secure, granular access to private applications hosted in on-premises data centers or private clouds. It can be achieved through two main methods: ZTNA (Zero Trust Network Access), which provides session-specific access based on identity and device posture, or through SD-WAN integration, where the FortiSASE cloud acts as a spoke connecting to a corporate SD-WAN Hub.

Why other options are incorrect:

Secure VPN Access (SVA) (Option D): While SASE uses VPN technology (SSL or IPsec) as a transport for the Endpoint mode, 'SVA' is not a formal curriculum-defined use case. The SASE framework is intended to evolve beyond traditional 'Secure VPN Access' into the SIA and SPA models.

Secure Browser Access (SBA) (Option E): Although FortiSASE offers Remote Browser Isolation (RBI), it is considered a feature or a component of the broader Secure Internet Access (SIA) use case rather than a separate, standalone use case in the core administrator curriculum.

Question 3

Question Type: MultipleChoice

An existing Fortinet SD-WAN customer who has recently deployed FortiSASE wants to have a comprehensive view of, and combined reports for, both SD-WAN branches and remote users. How can the customer achieve this?

Options:

A- Forward the logs from FortiSASE to Fortinet SOCaaS.
B- Forward the logs from FortiGate to FortiSASE.
C- Forward the logs from FortiSASE to the external FortiAnalyzer.
D- Forward the logs from the external SD-WAN FortiAnalyzer to FortiSASE.

Answer:

C

Explanation:

For customers with hybrid environments (on-premises SD-WAN branches and remote FortiSASE users), the FortiOS 7.6 and FortiSASE curriculum recommends centralized log aggregation for unified visibility.

Centralized Reporting: The standard architectural best practice is to forward logs from FortiSASE to an external FortiAnalyzer (Option C).

Unified View: Since the customer's on-premises FortiGate SD-WAN branches are already sending logs to an existing FortiAnalyzer, adding the FortiSASE log stream to that same FortiAnalyzer allows for the creation of combined reports.

Fabric Integration: This setup leverages the Security Fabric, enabling the FortiAnalyzer to provide a single pane of glass for monitoring security events, application usage, and SD-WAN performance metrics across the entire distributed network.

Why other options are incorrect:

Option A: SOCaaS is a managed service for threat monitoring, not a primary tool for an administrator to generate combined SD-WAN/SASE operational reports.

Option B: FortiSASE is not designed to act as a log collector or reporting hub for external on-premises FortiGates.

Option D: Data flows from the source (FortiSASE) to the collector (FortiAnalyzer), not the other way around.

Question 4

Question Type: MultipleChoice

You have a FortiGate configuration with three user-defined SD-WAN zones and one or two members in each of these zones. One SD-WAN member is no longer used in health-check and SD-WAN rules. This member is the only member of its zone. You want to delete it.

What happens if you delete the SD-WAN member from the FortiGate GUI?

Options:

A- FortiGate displays an error message. SD-WAN zones must contain at least one member.
B- FortiGate accepts the deletion and removes static routes as required.
C- FortiGate accepts the deletion with no further action.
D- FortiGate accepts the deletion and places the member in the default SD-WAN zone.

Answer:

B

Explanation:

Questions no: 9 Verified Answer: B

Comprehensive and Detailed Explanation with all FortiSASE and SD-WAN 7.6 Core Administrator curriculum documents: According to the SD-WAN 7.6 Core Administrator study guide and FortiOS 7.6 Administration Guide, the behavior for deleting an SD-WAN member from the GUI when it is the only member in its zone is governed by the following operational logic:

Reference Checks: Before allowing the deletion of any SD-WAN member, FortiOS performs a 'check for dependencies.' If an interface is being used in an active Performance SLA or an SD-WAN Rule, the GUI will typically prevent the deletion or gray out the option until those references are removed. However, the question specifies that this member is no longer used in health-checks or rules.

Zone Integrity: Unlike some other network objects, an SD-WAN zone is permitted to exist without any members. When you delete the final member of a user-defined zone through the GUI, the zone itself remains in the configuration as an empty container.

Route Management: When an SD-WAN member is deleted, any static routes that were specifically tied to that interface's membership in the SD-WAN bundle are automatically updated or removed by the FortiGate to prevent routing loops or 'black-holing' traffic. This is part of the automated cleanup process handled by the FortiOS management plane.

GUI vs. CLI: In the GUI, the process is streamlined to allow the removal of the member interface. Once the member is deleted, the interface returns to being a 'regular' system

interface and can be used for standard firewall policies or other functions.

Why other options are incorrect:

Option A: There is no requirement that a zone must contain at least one member; 'empty' zones are valid configuration objects in FortiOS 7.6.

Option C: While the deletion is accepted, it is not with 'no further action'---the system must still reconcile the routing table and interface status.

Option D: FortiGate does not automatically move deleted members into the default zone (virtual-wan-link). Once deleted, the interface is simply no longer an SD-WAN member.

Question 5

Question Type: MultipleChoice

Which configuration is a valid use case for FortiSASE features in supporting remote users?

Options:

A- Enabling secure SaaS access through SD-WAN integration, protecting against web-based threats with data loss prevention, and monitoring user connectivity with shadow IT visibility.
B- Monitoring SaaS application performance, isolating browser sessions for all websites, and integrating with SD-WAN for data loss prevention.
C- Enabling secure web browsing to protect against threats, providing explicit application access with zero-trust or SD-WAN integration, and addressing shadow IT visibility with data loss prevention.
D- Providing secure web browsing through remote browser isolation, addressing shadow IT with zero-trust access, and protecting data at rest only.

Answer:

C

Explanation:

According to the FortiSASE 7.6 Architecture Guide and FCP - FortiSASE 24/25 Administrator materials, the solution is built around three primary use cases that support a hybrid workforce:

Secure Internet Access (SIA): This enables secure web browsing by applying security profiles such as Web Filter, Anti-Malware, and SSL Inspection in the SASE cloud. It protects remote users from internet-based threats regardless of their location.

Secure Private Access (SPA): This provides granular, explicit access to private applications hosted in data centers or the cloud. It is achieved through ZTNA (Zero Trust Network Access) for session-based security or through SD-WAN integration where FortiSASE acts as a spoke to an existing corporate SD-WAN hub.

SaaS Security: FortiSASE utilizes Inline-CASB and Shadow IT visibility to monitor and control the use of cloud applications. Data Loss Prevention (DLP) is integrated into these workflows to prevent sensitive corporate data from being uploaded to unauthorized SaaS platforms.

Why other options are incorrect:

Option A: While it mentions SD-WAN and Shadow IT, it misses the core definition of SIA (secure web browsing) which is the primary driver for SASE deployments.

Option B: Remote Browser Isolation (RBI) is typically applied to risky or uncategorized websites, not 'all websites,' due to the high performance and resource overhead.

Option D: FortiSASE is designed to protect data in motion (via security profiles) as well as data stored in sanctioned cloud apps, not 'at rest only'.

Question 6

Question Type: MultipleChoice

Which three reports are valid report types in FortiSASE? (Choose three.)

Options:

A- Web Usage Summary Report
B- Endpoint Compliance Deviation Report
C- Vulnerability Assessment Report
D- Shadow IT Report
E- Cyber Threat Assessment

Answer:

A, C, D

Explanation:

According to the FortiSASE 7.6 Administration Guide and the FCP - FortiSASE 24/25 training materials, FortiSASE leverages a cloud-native FortiAnalyzer instance to provide specialized reports. These reports are designed to give administrators visibility into remote user behavior,

endpoint health, and cloud application usage.

The three valid and standard report types available directly within the FortiSASE portal are:

Web Usage Summary Report (Option A): This report provides a high-level overview of web activity across the SASE deployment. It categorizes traffic by website categories (e.g., Social Media, Streaming, Malicious Sites), top users by bandwidth, and blocked requests, helping IT teams understand how internet resources are being consumed by remote workers.

Vulnerability Assessment Report (Option C): Since FortiSASE integrates with FortiClient and an embedded EMS, it can aggregate vulnerability scan data from managed endpoints. This report lists software vulnerabilities found on user devices (OS-level and application-level), providing a 'Security Rating' or posture assessment that is critical for Zero Trust Network Access (ZTNA) enforcement.

Shadow IT Report (Option D): Leveraging the built-in CASB (Cloud Access Security Broker) capabilities, this report identifies 'unsanctioned' or 'risky' SaaS applications being used by employees. It helps organizations discover hidden security risks by cataloging cloud applications that have not been explicitly approved by the IT department.

Why other options are incorrect:

Endpoint Compliance Deviation Report (Option B): While FortiSASE performs compliance checks via ZTNA tags, this specific name is not a standard 'Report Type' template in the portal; compliance is typically monitored via the Endpoint Management or ZTNA Dashboards.

Cyber Threat Assessment (Option E): The Cyber Threat Assessment Program (CTAP) is a specific Fortinet sales and auditing tool used to generate a one-time report on a network's security posture (often used for FortiGate evaluations). It is not a native, recurring report type within the day-to-day FortiSASE administration interface.

Question 7

Question Type: MultipleChoice

How is the Geofencing feature used in FortiSASE? (Select one answer)

Options:

A- To allow or block remote user connections to FortiSASE POPs from specific countries.
B- To restrict access to applications based on the time of day in specific countries.
C- To encrypt data at rest on mobile devices in specific countries.
D- To monitor user behavior on websites and block non-work-related content from specific countries

Answer:

A

Explanation:

According to the FortiSASE 7.6 Administration Guide and the FCP - FortiSASE 24/25 Administrator study materials, the Geofencing feature is a security measure implemented at the edge of the FortiSASE cloud to control ingress connectivity based on the physical location of the user.

Access Control by Location (Option A): Geofencing allows administrators to allow or block remote user connections to the FortiSASE Points of Presence (PoPs) based on the source country, region, or specific network infrastructure (e.g., AWS, Azure, GCP).

Scope of Application: This feature is universal across all SASE connectivity methods. It applies to Agent-based users (FortiClient), Agentless users (SWG/PAC file), and Edge devices (FortiExtender/FortiAP). If a user attempts to connect from a blacklisted country, the connection is dropped at the PoP level before the user can even attempt to authenticate.

Use Case Example: An organization operating exclusively in North America might configure geofencing to block all connections originating from outside the US and Canada. This significantly reduces the attack surface by preventing brute-force or unauthorized access attempts from high-risk regions or countries where the organization has no legitimate employees.

Configuration Path: In the FortiSASE portal, this is managed under Configuration > Geofencing. From there, administrators can create an 'Allow' or 'Deny' list and select the relevant countries from a standardized global database.

Why other options are incorrect:

Option B: While FortiSASE supports Time-based schedules for firewall policies, geofencing is specifically an IP-to-Geography mapping tool for connection admission, not a time-of-day restriction tool.

Option C: Encryption of data at rest on mobile devices is a function of an MDM (Mobile Device Management) solution or local OS features (like FileVault or BitLocker), not a SASE network geofencing feature.

Option D: Monitoring web behavior and blocking non-work content is the role of the Web Filter and Application Control profiles, which operate on the traffic after the connection is allowed by geofencing.

Question 8

Question Type: MultipleChoice

Which two statements about configuring a steering bypass destination in FortiSASE are correct? (Choose two.)

Options:

A- Subnet is the only destination type that supports the Apply condition
B- Apply condition allows split tunneling destinations to ae applied to On-net. off-net. or both types of endpoints
C- You can select from four destination types: Infrastructure, FQDN, Local Application, or Subnet
D- Apply condition can be set only to On-net or Off-net. but not both

Answer:

B, C

Explanation:

According to the FortiSASE 7.6 Feature Administration Guide, steering bypass destinations (also known as split tunneling) allow administrators to optimize bandwidth by redirecting specific trusted traffic away from the SASE tunnel to the endpoint's local physical interface.

Destination Types (Option C): When creating a bypass destination, administrators can select from four distinct types: Infrastructure (pre-defined apps like Zoom/O365), FQDN (specific domains), Local Application (identifying processes on the laptop), or Subnet (specific IP ranges).

Apply Condition (Option B): The 'Apply' condition is a flexible setting that allows the administrator to choose when the bypass is active. It can be applied to endpoints that are On-net (inside the office), Off-net (remote), or Both. This ensures that if a user is in the office, they don't use the SASE tunnel for local resources, but if they are home, they might still bypass high-bandwidth sites like YouTube to preserve tunnel capacity.

Why other options are incorrect:

Option A: Subnet is one of four types and is not the only type supporting these conditions.

Option D: The system explicitly supports 'Both' to ensure consistency across network transitions.