Prepare Smart for Success Free Fortinet NSE7_SSE_AD-25 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 7 - FortiSASE 25 Enterprise Administrator exam PDF questions now. Get authentic NSE7_SSE_AD-25 dumps packed with verified answers and secure your certification success with PrepBolt NSE7_SSE_AD-25 exam pdf questions and answers.

Thank you for Downloading NSE7_SSE_AD-25 exam PDF Demo

https://prepbolt.com/NSE7_SSE_AD-25.html

Question 1

Question Type: MultipleChoice

How does FortiSASE address the market trends of multicloud and Software-as-a-Service (SaaS) adoption, hybrid workforce, and zero trust? (Choose one answer)

Options:

A- It focuses solely on securing on-premises networks, ignoring cloud and remote work challenges.
B- It prioritizes legacy VPN connections for hybrid workforces, bypassing modern cloud and zero-trust security measures.
C- It provides visibility and control for multicloud and SaaS environments, ensures secure and seamless access for hybrid workforces, and implements zero-trust principles.1
D- It supports only zero-trust frameworks without addressing multicloud or hybrid workforce needs.

Answer:

C

Explanation:

FortiSASE is designed as a unified, single-vendor solution that specifically targets the convergence of networking and security to address the modern challenges of a distributed enterprise.2

Multicloud and SaaS Adoption: FortiSASE addresses the surge in cloud-first strategies by providing Next-Generation Dual-Mode CASB (Cloud Access Security Broker).3 This feature uses both inline and API-based inspection to provide comprehensive visibility into sanctioned and unsanctioned SaaS applications (Shadow IT), ensuring that data is protected regardless of whether it resides in AWS, Azure, Google Cloud, or SaaS platforms like Microsoft 365.

Hybrid Workforce: To support a workforce that moves between the home, the office, and public spaces, FortiSASE delivers consistent security posture.5 It replaces the inconsistent experience of legacy VPNs with a geographically dispersed network of over 150 Points of Presence (PoPs), ensuring low-latency access to applications while maintaining high-performance SSL inspection and threat detection for all remote users.

Zero Trust Integration: Central to the FortiSASE architecture is Universal ZTNA (Zero Trust Network Access).7 Unlike traditional VPNs that grant broad network access, ZTNA applies the principle of 'never trust, always verify'. It grants access on a per-session, per-application basis, continuously verifying the device posture and user identity before and during application access.9 This shift from implicit to explicit trust significantly reduces the internal attack surface and mitigates the risk of lateral movement by attackers.

By integrating these components into a single operating system (FortiOS) and managed via a single

console, FortiSASE simplifies IT operations while delivering the visibility and control required for today's multicloud and hybrid environments.

Question 2

Question Type: MultipleChoice

Which service is included in a secure access service edge (SASE) solution, but not in a security service edge (SSE) solution? (Choose one answer)

Options:

A- SWG
B- SD-WAN1
C- CASB
D- ZTNA

Answer:

B

Explanation:

The distinction between SASE (Secure Access Service Edge) and SSE (Security Service Edge) is a fundamental architectural concept in modern networking and security.

SASE Definition: SASE is a comprehensive framework that converges networking capabilities (specifically SD-WAN) with cloud-native security services (SSE) into a single, unified service model.

SSE Definition: SSE represents the security-focused subset of SASE.4 It encompasses the core security pillars required for secure access, including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Zero Trust Network Access (ZTNA).

The Key Differentiator: While both solutions share the same security stack (SWG, CASB, ZTNA), SD-WAN (Software-Defined Wide Area Network) is the specific networking component that exists in a full SASE solution to provide intelligent path selection and optimized connectivity. SSE intentionally excludes these wide-area networking functions, focusing purely on the security service delivery layer.

According to the FortiSASE 25 Enterprise Administrator Study Guide, organizations that already have a robust networking infrastructure and only require a cloud-delivered security overlay would opt for SSE, whereas those seeking a complete transformation of both network and security would deploy a full SASE solution that includes SD-WAN.

Question 3

Question Type: MultipleChoice

You are configuring FortiSASE SSL deep inspection. What is required for FortiSASE to inspect encrypted traffic? (Choose one answer)

Options:

A- FortiSASE uses a third-party CA certificate without importing it to client machines, and SSL deep inspection supports only web filtering and application control.
B- FortiSASE acts as a root CA without needing a certificate, and SSL deep inspection is used only for split DNS and video filtering.
C- FortiSASE requires an external CA to issue certificates to client machines, and SSL deep inspection supports only antivirus and file filter.
D- FortiSASE acts as a certificate authority (CA) with a self-signed or internal CA certificate, requiring the root CA certificate to be imported into client machines.

Answer:

D

Explanation:

SSL deep inspection (DPI) is a critical security function that allows FortiSASE to decrypt and inspect the actual payload of encrypted traffic (such as HTTPS, SMTPS, and FTPS) to identify and block hidden threats.

The Role of the CA: For this process to occur, FortiSASE must act as a 'man-in-the-middle' by intercepting the SSL session, decrypting it for inspection, and then re-encrypting it before sending it to the endpoint.2 To re-encrypt the traffic, FortiSASE acts as a Certificate Authority (CA) and signs a new certificate for the destination website on the fly.

Certificate Types: This CA role can be fulfilled using the default self-signed certificate provided by Fortinet (typically Fortinet_CA_SSL) or a certificate issued by an organization's internal/private CA. Publicly trusted third-party CAs (like DigiCert or Let's Encrypt) do not sell CA-capable certificates that can be used for this type of inspection.

Client Machine Requirement: Because the endpoint's browser or operating system will not natively trust a certificate signed by a private or self-signed CA, the root CA certificate must be imported into the Trusted Root Certification Authorities store on all managed client machines. Failure to do so results in persistent certificate warnings or blocked connections for the end user.

Supported Features: Once enabled, SSL deep inspection provides the necessary visibility for high-level

security features to function, including Antivirus, Web Filtering, Data Loss Prevention (DLP), File Filter, and Application Control.

Question 4

Question Type: MultipleChoice

What is required to enable the MSSP feature on FortiSASE? (Choose one answer)

Options:

A- Multi-tenancy must be enabled on the FortiSASE portal.
B- MSSP user accounts and permissions must be configured on the FortiSASE portal.
C- The MSSP add-on license must be applied to FortiSASE.
D- Role-based access control (RBAC) must be assigned to identity and access management (IAM) users using the FortiCloud IAM portal.

Answer:

D

Explanation:

To enable the Managed Security Service Provider (MSSP) feature on FortiSASE, the administrative framework must be established outside of the local SASE instance within the broader FortiCloud ecosystem.

FortiCloud IAM Integration: The FortiSASE MSSP portal relies on FortiCloud Identity & Access Management (IAM) to define the scope of management for internal teams. Administrators do not create local 'MSSP users' within the SASE portal itself; instead, they must use the FortiCloud IAM portal to assign specific Role-Based Access Control (RBAC) to IAM users.

Permissions and Scope: These RBAC settings determine which customer tenants (Organizational Units or OUs) an MSSP administrator can view, configure, or monitor. Without the proper role assignment in the IAM portal, the MSSP portal and its multi-tenant viewing capabilities will not be accessible to the user, even if the account has the necessary licenses.

Hierarchical Management: Once RBAC is correctly assigned, the MSSP administrator can leverage the FortiCloud Organizations service to manage multiple customer accounts from a single pane of glass. This centralized approach ensures that security policies and configurations can be standardized across the entire customer base while maintaining strict data isolation between tenants.

According to the FortiSASE 25 Multitenant Deployment Guide, configuring the IAM portal is the primary

prerequisite that grants an MSSP internal team the permissions necessary to perform operations on customer FortiSASE tenants.

Question 5

Question Type: MultipleChoice

Which two statements about FortiSASE Geofencing with regional compliance are true? (Choose two answers)

Options:

A- You can configure regional compliance on the security POP or the on-premises device, not both.1
B- If no regional compliance rule is configured, the connection is made to the closest security POP.
C- A regional compliance rule can connect only to an on-premises device or only to a security POP.2
D- The connection order for a regional compliance rule is always the security POP first, followed by the on-premises device.

Answer:

B, C

Explanation:

FortiSASE Geofencing and Regional Compliance allow administrators to control where remote users connect based on their physical location, which is determined by the endpoint's public IP address.3

Default Connection Behavior: By default, FortiSASE uses a 'best-effort' geolocation logic to ensure the lowest latency for the user. If an administrator has not configured a specific regional compliance rule for a user's country or region, FortiClient will automatically attempt to connect to the closest available FortiSASE security PoP (Point of Presence) based on proximity.4

Regional Compliance Rules: When an organization must enforce data residency or specific security routing requirements, they create Regional Compliance rules. According to the FortiSASE 25 Feature Administration Guide, these rules allow the administrator to override the default 'closest PoP' behavior for specific countries.

Connectivity Options: Within a regional compliance rule, the administrator must specify the destination for the traffic. The system provides a choice between two distinct connection types: a FortiSASE Security PoP or an On-premises device (such as a FortiGate acting as a gateway).5 The documentation specifies that a rule is designed to point to one of these types at a time to satisfy the compliance requirement for that specific region.

Connection Priority: While multiple connections can be managed in a priority table, the logic for Regional Compliance is focused on directing the user to the designated compliant entry point. Option D is incorrect because the connection order is determined by the Priority and custom fail-over connections table; an administrator can manually adjust the sequence, so it is not 'always' the security PoP first.

Question 6

Question Type: MultipleChoice

Which two statements about the Hub Selection Method in FortiSASE Secure Private Access (SPA) are correct? (Choose two answers)

Options:

A- When using Hub Health and Priority, FortiSASE selects the highest priority hub that meets the configured SLA thresholds.
B- When using BGP MED, FortiSASE selects the hub with the lowest MED value only if it also meets the configured SLA thresholds.
C- When using SLA thresholds, administrators can customize latency, jitter, and packet loss for each security POP.
D- When using Hub Health and Priority, all hubs with the same priority are always selected regardless of SLA results.

Answer:

A, B

Explanation:

According to the NSE7 SASE Enterprise Guide (Pages 64 & 153), FortiSASE utilizes an intelligent engine to manage connectivity to private resources through various selection methods:

Hub Health and Priority: FortiSASE incorporates a built-in SD-WAN engine for intelligent routing selection among established IPsec links. The health check IP address periodically receives performance metrics, including jitter, latency, and packet loss, for each service connection. In this mode, FortiSASE evaluates the available hubs and selects the one with the highest priority (the most preferred value) within each POP, provided that the hub meets the defined service-level agreement (SLA) requirements. For this configuration to function correctly, both FortiSASE and the SPA hub must use the same Autonomous System Number (ASN).

BGP Multiple Exit Discriminator (MED): This method leverages the standard BGP MED attribute, which

allows an autonomous system to signal its preferred entry point to a peer. FortiSASE learns the MED values advertised by the configured hubs. The architecture is designed so that the lower the MED value, the more preferred the path is to the receiving router. Consistent with the 'Zero Trust' and 'Secure Access' principles, even when using BGP MED, the selection is gated by the health engine; therefore, the hub is only selected if it also satisfies the configured SLA thresholds.

While SLA thresholds can be configured, the primary logic for hub selection focuses on how priority and dynamic routing attributes (like MED) interact with the real-time health of the tunnel.

Thank You for trying NSE7_SSE_AD-25 PDF Demo

To try our NSE7_SSE_AD-25 practice exam software visit link below

https://prepbolt.com/NSE7_SSE_AD-25.html

Start Your NSE7_SSE_AD-25 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE7_SSE_AD-25 preparation with actual exam questions.