Passcert

Higher Quality, better service!

Q&A

Http://www.passcert.com

We offer free update service for one year.

Exam : **NSE7_SSE_AR-26**

Title : Fortinet NSE 7 - SASE 26 Architect

Version : DEMO

1.(Single Choice - Architecture & POP Selection)
In a FortiSASE Agent-based deployment, how does FortiClient dynamically select and connect to the nearest security POP when a user travels to a different country?
A. FortiClient actively probes all known global POPs via ICMP during initialization and selects the node returning the lowest latency metrics.
B. It relies on the Fortinet Anycast DNS service, which dynamically returns the optimal POP IP based on the source geolocation of the request.
C. It downloads a pre-configured static POP list pushed by FortiClient EMS, attempting connections sequentially from top to bottom until successful.
D. The corporate FortiManager continuously calculates and pushes the most current optimal POP routing mapping table directly to all active endpoints.
Answer: B
Explanation:
Why B is correct: This is the core mechanism of the FortiSASE globally distributed architecture. FortiSASE relies on Anycast DNS technology. When FortiClient attempts to resolve the cloud gateway domain name, the Anycast network automatically routes the DNS request to the geographically or topologically nearest Fortinet DNS server, returning the IP address of the closest SASE POP node.
Why A, C, D are incorrect: ICMP probing is slow and often blocked by ISPs. Static lists cannot facilitate dynamic global roaming. FortiManager handles configuration management, not real-time endpoint traffic distribution.

2.(Multiple Choice - SAML SSO Troubleshooting)
You are configuring SAML SSO integration between FortiSASE and Azure AD (IdP). After completing the configuration, users experience an "infinite loop" of redirects upon logging in and cannot access the system.
Which TWO misconfigurations would cause this specific issue? (Choose two)
A. The IdP Entity ID configured on the FortiSASE service provider portal does not perfectly match the Entity ID string provided by Azure AD.
B. The Assertion Consumer Service (ACS) URL configured on the Azure AD portal contains a typographical error or a protocol port mismatch.
C. The Azure AD enterprise application configuration is currently missing the mandatory User Principal Name (UPN) SAML claim mapping.
D. The designated user groups within the FortiSASE authentication settings have not been properly bound to the local user credentials database.
Answer: A, B
Explanation:
Why A, B are correct: In SAML troubleshooting, an infinite loop (SSO Loop) typically occurs when the Service Provider (SP - FortiSASE) fails to validate the response from the Identity Provider (IdP), repeatedly forcing re-authentication. The most common causes are foundational SAML trust parameter mismatches: an Entity ID mismatch (SP rejects the IdP), or an ACS URL error (IdP sends the token to the wrong destination, and the SP, waiting for a token, redirects again).
Why C is incorrect: UPN mapping errors usually lead to successful authentication but failed authorization (logging in but having no valid profile), rather than an infinite redirect loop.
Why D is incorrect: In a SAML SSO environment, authentication is delegated entirely to the IdP; local

passwords are not bound in FortiSASE.

3.(Single Choice - ZTNA Architecture Integration)
An organization has deployed FortiSASE Secure Private Access (SPA). An administrator notices that users can successfully establish IPsec tunnels, but they fail to match any ZTNA access rules, resulting in all internal application traffic being blocked. Checking the FortiSASE console reveals that the user endpoints have no dynamic Tags assigned.
What is the most likely cause of this issue?
A. The user's endpoint FortiClient has not yet successfully requested and obtained a valid ZTNA client certificate from the certificate authority.
B. FortiSASE has not established an authorized and functioning Security Fabric synchronization connection with the enterprise FortiClient EMS.
C. The backend BGP neighbor relationship associated with the SPA tunnel is not correctly redistributing the necessary internal subnet routes.
D. The global SSL Deep Inspection profile has been accidentally enforced within the FortiSASE default outbound internet firewall policies.
Answer: B
Explanation:
Why B is correct: The core of ZTNA involves the EMS evaluating endpoint posture and generating Tags. If FortiSASE displays no tags, it means FortiSASE is not syncing the tag database with EMS via the Security Fabric. Without tags, the ZTNA engine cannot match any policies.
Why A is incorrect: Certificates are used for device identification and encryption. A missing certificate would drop the connection entirely, which does not explain why the tunnel is up but "no tags" are visible on the console.
Why C, D are incorrect: Routing and deep inspection relate to network connectivity and payload filtering, respectively. They are entirely separate from the ZTNA tag generation and synchronization mechanics.

4.(Drag and Drop /Matching)
Match the following key components in a FortiSASE SPA architecture to their core networking functions.
Components:
1. FortiClient
2. FortiSASE Security PoP
3. FortiGate Hub (Enterprise)
4. FortiClient EMS
Functions:
A. Terminates IPsec tunnels from the cloud, establishes Overlay connectivity, and advertises corporate internal routes to the cloud.
B. Performs endpoint posture checks and generates/distributes dynamic ZTNA tags.
C. Intercepts and proxies end-user traffic, establishing the first-hop secure encrypted connection.
D. Enforces the organization's unified cloud security policies (e.g., Web Filtering, DLP, IPS).
Answer: 1-C, 2-D, 3-A, 4-B
Explanation:
FortiClient (1-C): Resides on the endpoint, capturing traffic and building the tunnel to the nearest POP.
FortiSASE PoP (2-D): The cloud gateway hosting the Security Stack and enforcing filtering policies.

FortiGate Hub (3-A): Deployed in the enterprise data center, acting as the SPA Hub to receive POP tunnels and exchange routing. FortiClient EMS (4-B): Endpoint management server responsible for compliance checks and ZTNA tagging logic.

5.(Multiple Choice - SPA Redundancy and SD-WAN)
When designing a dual-Hub redundant FortiSASE SPA architecture (Primary and Disaster Recovery Data Centers), an administrator wants to ensure that if the Primary Hub experiences severe jitter or high latency, cloud traffic automatically and seamlessly fails over to the DR Hub.
Which TWO core features must be configured on the FortiSASE side? (Choose two)
A. Configure active Performance SLAs (health checks) targeting the remote gateways for both of the established SPA IPsec tunnels.
B. Configure a global SD-WAN rule with the traffic steering strategy explicitly set to the "Maximize Bandwidth" operational mode.
C. Configure a dynamic SD-WAN rule with the traffic steering strategy set to either the "Lowest Cost (SLA)" or "Best Quality" mode.
D. Enable the Route Reflector capability within the BGP routing configuration associated with both of the enterprise SPA tunnels.
Answer: A, C
Explanation:
Why A, C are correct: In the FortiOS architecture (which powers FortiSASE), dynamic routing based on link quality requires a two-part combination. First, a Performance SLA (probe) must continuously measure Latency, Jitter, and Packet Loss. Second, an SD-WAN Rule must reference this SLA, utilizing either a Lowest Cost (meets thresholds) or Best Quality (always picks the best performing link) strategy for traffic steering.
Why B is incorrect: "Maximize Bandwidth" is an ECMP load-balancing strategy and cannot facilitate active failover based on specific link quality degradation (like jitter).
Why D is incorrect: Route Reflectors are used in large-scale BGP topologies to solve IBGP full-mesh requirements and are unrelated to dynamic, quality-based failover.