PassQueen
a.k.a dumpsqueen.com

FCSS FortiSASE 23 Administrator

Fortinet FCSS_SASE_AD-23

Version Demo

Total Demo Questions: 5

Total Premium Questions: 52

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, FortiSASE deployment	10
Topic 2, Endpoint management	9
Topic 3, Secure internet access	12
Topic 4, Secure private access	12
Topic 5, Secure SaaS access	3
Topic 6, Monitoring and reporting	6
Total	52

QUESTION NO: 1

During initial tenant activation, an organization plans to deploy managed FortiClient endpoints in a required service region and wants remote users to connect through a nearby FortiSASE service edge.

Which two FortiSASE location selections are relevant to these requirements? (Choose two.)

A. Endpoint management

B. Points of presence

C. Authentication

D. SD-WAN hub

E. Logging

ANSWER: A B

Explanation:

Endpoint management and **Points of presence** are correct. The endpoint-management location determines the regional service used to manage FortiClient endpoints and related endpoint capabilities. The points-of-presence selection determines the FortiSASE cloud service edge through which users and sites receive cloud-delivered security services.

Logging location is important for log storage and analytics, but it does not select the endpoint-management service or the user-facing security PoP. Authentication and SD-WAN hub are not initial FortiSASE data-center location components.

QUESTION NO: 2

How does FortiSASE hide user information when viewing and analyzing logs?

A. By hashing data using Blowfish

B. By hashing data using salt

C. By encrypting data using Secure Hash Algorithm 256-bit (SHA-256)

D. By encrypting data using advanced encryption standard (AES)

ANSWER: B

Explanation:

FortiSASE hides user information in log views and analytics by hashing the relevant data using salt. Salted hashing transforms identifying values into non-readable, consistent pseudonymous values for the applicable scope, allowing administrators to correlate events associated with the same user without directly exposing that user's original identifying information. The salt is important because it adds an additional value to the hashing process, strengthening privacy protection and reducing the usefulness of precomputed hash lookups against common identifiers. This supports operational log investigation while applying privacy controls to sensitive user-related data.

In FortiSASE, logging and analytics are cloud-delivered capabilities, so protecting identity-related information displayed during monitoring is particularly important for organizations that must limit access to personally identifiable information. The salted-hash approach provides obfuscation for log analysis rather than attempting to use an encryption algorithm as the privacy mechanism described in this feature. Fortinet's FortiSASE Administration Guide documents the platform's administration, monitoring, and logging capabilities; consult the current guide for release-specific behavior and configuration details. See the FortiSASE documentation portal and the FortiSASE 23.2 Administration Guide.

QUESTION NO: 3

An organization uses Secure Private Access (SPA) so that its corporate FortiGate can receive endpoint information from FortiSASE.

Which three configuration actions are required to establish this integration? (Choose three.)

A. Add the FortiGate IP address to the secure private access configuration.

B. Configure the FortiClient EMS cloud connector on the FortiGate.

C. Register the FortiGate and FortiSASE under the same FortiCloud account.

D. Authorize the FortiGate as a ZTNA access proxy.

E. Install a FortiSASE ZTNA license on the FortiGate.

ANSWER: A B C

Explanation:

The FortiGate address must be added to the SPA configuration so that FortiSASE identifies the participating corporate firewall. The FortiGate uses the FortiClient EMS cloud connector to connect to FortiSASE and consume endpoint information. In addition, the FortiGate and FortiSASE tenant must be registered under the same FortiCloud account. A ZTNA access proxy and a FortiGate ZTNA license are not requirements for the SPA endpoint-information integration.

QUESTION NO: 4

A customer wants to upgrade their legacy on-premises proxy to a could-based proxy for a hybrid network. Which FortiSASE features would help the customer to achieve this outcome?

A. SD-WAN and NGFW

B. SD-WAN and inline-CASB

C. zero trust network access (ZTNA) and next generation firewall (NGFW)

D. secure web gateway (SWG) and inline-CASB

ANSWER: D

Explanation:

The correct feature combination is **secure web gateway (SWG) and inline-CASB**. FortiSASE Secure Web Gateway provides a cloud-delivered security enforcement point for internet-bound web traffic. It enables organizations to move web-proxy functions from an on-premises appliance to Fortinet's SASE cloud, where traffic can be inspected and controlled consistently for users connecting from branch locations, remote sites, and other hybrid-work environments. SWG policies can apply web filtering, SSL inspection, application control, and threat protection before users reach internet destinations.

Inline Cloud Access Security Broker capabilities complement SWG by identifying and governing the use of cloud applications in real time. This is particularly important when replacing a traditional proxy because modern web traffic is frequently directed to SaaS services rather than conventional websites. Inline-CASB gives administrators visibility into sanctioned and unsanctioned cloud application activity and supports policy enforcement to control cloud usage and help protect sensitive data. Together, these services provide the cloud-based web access security and SaaS control needed for a hybrid network without depending on a legacy on-premises proxy. Fortinet describes these cloud-delivered security functions in its FortiSASE documentation and on the FortiSASE product page.

QUESTION NO: 5

When you configure FortiSASE Secure Private Access (SPA) with SD-WAN integration, you must establish a routing adjacency between FortiSASE and the FortiGate SD-WAN hub. Which routing protocol must you use?

A. BGP

B. IS-IS

C. OSPF

D. EIGRP

ANSWER: A

Explanation:

BGP is required to establish the dynamic routing adjacency between FortiSASE Secure Private Access and the FortiGate SD-WAN hub. In this design, FortiSASE and the hub form a BGP peer relationship across the SPA/IPsec connectivity. The adjacency lets each side advertise the networks it can reach and learn routes from the other side automatically. As a result, traffic for private applications and protected internal subnets can be routed through the appropriate FortiSASE or SD-WAN path without relying on a static-route-only design.

BGP is especially suited to this integration because it provides controlled route exchange between the FortiSASE cloud service and the customer's SD-WAN hub. Route advertisement, filtering, attributes, and failover behavior can be managed centrally at the hub while FortiSASE receives the reachable private-prefix information needed to steer user traffic to private resources. This dynamic exchange also supports resilient operation when tunnel or hub-path availability changes, allowing routing to converge based on the established BGP session and advertised prefixes.

Fortinet documents SPA SD-WAN integration and its routing configuration in the FortiSASE Administration Guide. General FortiGate BGP configuration and routing behavior are documented in the FortiGate Administration Guide: BGP.