KillTest

Mejor calidad. Mejor servicio

Preguntas de práctica

https://www.killtest.es

Actualizaciones gratuitas durante un año

Exam : **FCSS_SASE_AD-25**

Title : FCSS - FortiSASE 25 Administrator

Version : DEMO

1.In the Secure Private Access (SPA) use case, which two FortiSASE features facilitate access to corporate applications? (Choose two.)
A. cloud access security broker (CASB)
B. SD-WAN
C. zero trust network access (ZTNA)
D. thin edge
Answer: B,C
Explanation:
SD-WAN allows efficient and secure routing of traffic from users to corporate applications, while ZTNA enables secure access control and verification for users connecting to internal resources, both of which are essential for Secure Private Access (SPA) in FortiSASE.

2.Which two components are part of onboarding a secure web gateway (SWG) endpoint for secure internet access (SIA)? (Choose two.)
A. proxy auto-configuration (PAC) file
B. FortiSASE certificate authority (CA) certificate
C. FortiClient software
D. tunnel policy
Answer: A,C
Explanation:
A PAC file is used to redirect client web traffic through the SWG, and FortiClient software is required to connect endpoints to the FortiSASE service for secure internet access (SIA).

3.Which two advantages does FortiSASE bring to businesses with microbranch offices that have FortiAP deployed for unmanaged devices? (Choose two.)
A. It secures internet access both on and off the network.
B. It uses zero trust network access (ZTNA) tags to perform device compliance checks.
C. It eliminates the requirement for an on-premises firewall.
D. It simplifies management and provisioning.
Answer: A,C

4.Which information can an administrator monitor using reports generated on FortiSASE?
A. sanctioned and unsanctioned Software-as-a-Service (SaaS) applications usage
B. FortiClient vulnerability assessment
C. SD-WAN performance
D. FortiSASE administrator and system events
Answer: A
Explanation:
FortiSASE reporting provides visibility into the usage of sanctioned and unsanctioned SaaS applications, enabling administrators to monitor cloud application activity and enforce security policies.

5.In a FortiSASE secure web gateway (SWG) deployment, which two features protect against web-based threats? (Choose two.)
A. SSL deep inspection for encrypted web traffic

B. malware protection with sandboxing capabilities
C. web application firewall (WAF) for web applications
D. intrusion prevention system (IPS) for web traffic
Answer: A,B
Explanation:
SSL deep inspection allows FortiSASE to analyze encrypted web traffic for threats, while malware protection with sandboxing detects and blocks malicious files delivered through web channels.