FCSSFortiSASE 25 Administrator

Fortinet FCSS_SASE_AD-25

Version Demo

Total Demo Questions: 7

Total Premium Questions: 73

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to FortiSASE	6
Topic 2, Initial Configuration	12
Topic 3, Secure Internet Access	16
Topic 4, Secure Private Access	12
Topic 5, Endpoint Security	16
Topic 6, Monitoring and Troubleshooting	11
Total	73

QUESTION NO: 1

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 for encrypted web traffic is a key SWG protection because much modern web traffic uses HTTPS. After the endpoint trusts the organization's inspection certificate, FortiSASE can decrypt the applicable traffic, inspect the content and session, apply security policies, and then re-encrypt it. This provides visibility needed to identify threats that would otherwise be concealed within encrypted web sessions.

Malware protection with sandboxing capabilities protects users from malicious files obtained through websites, downloads, and other browser-delivered content. Antivirus scanning can identify known malicious content, while sandbox analysis provides an additional layer for suspicious or previously unknown files by observing their behavior in an isolated environment. This layered approach helps prevent malware from reaching endpoints through web access and supports FortiSASE's cloud-delivered security inspection model. Fortinet describes FortiSASE as combining secure web access with integrated security services, including threat protection, and documents sandboxing as a mechanism for analyzing suspicious files. See FortiSASE product information and FortiSandbox information.

QUESTION NO: 2

What is the benefit of SD-WAN on-ramp deployment with FortiSASE?

A. To provide access to private applications using the bookmark portal

B. To provide device compliance checks using ZTNA tags

C. To secure internet traffic for branch users

D. To manage branch location endpoints

ANSWER: C

Explanation:

To secure internet traffic for branch users is the key benefit of an SD-WAN on-ramp deployment with FortiSASE. In this model, a FortiGate appliance at the branch establishes secure connectivity to the FortiSASE cloud and steers eligible internet-bound traffic through the service. FortiSASE then applies centralized cloud-delivered security controls, such as secure web gateway inspection, firewall policies, intrusion prevention, and web filtering, before traffic reaches the internet. This allows organizations to enforce a consistent security posture for branch users regardless of the branch's physical location or its local internet connection. SD-WAN capabilities also enable intelligent path selection and traffic steering, helping ensure that traffic intended for FortiSASE follows the appropriate secure overlay path. Rather than requiring every branch to deploy and maintain a full set of independently managed security services, administrators can use FortiSASE policy enforcement centrally while retaining FortiGate's branch networking and SD-WAN functions. Fortinet describes this use case as connecting branches to FortiSASE through SD-WAN for secure internet access and consistent protection. See the FortiSASE Administration Guide: SD-WAN on-ramp and the FortiSASE product overview.

QUESTION NO: 3

Which two are required to enable central management on FortiSASE? (Choose two.)

A. FortiSASE connector configured on FortiManager.

B. FortiSASE central management entitlement applied to FortiManager.

C. The FortiManager IP address in the FortiSASE central management configuration.

D. FortiManager and FortiSASE registered under the same FortiCloud account.

ANSWER: B D

Explanation:

Enabling FortiSASE central management requires an applicable FortiSASE central-management entitlement on FortiManager and a common FortiCloud account registration for FortiManager and the FortiSASE tenant. The entitlement authorizes the FortiManager instance to manage FortiSASE through the FortiCloud service; without it, the central-management capability is not available for activation. The shared FortiCloud account establishes the required ownership and service association between the management platform and the FortiSASE instance. This lets FortiCloud validate that the FortiManager appliance is authorized to discover, connect to, and centrally administer that tenant. Consequently, the entitlement must be applied to FortiManager, and both products must be registered to the same FortiCloud account before the central-management workflow can be completed. These prerequisites align with Fortinet's cloud-based licensing and tenant-association model for FortiSASE management. Consult the FortiSASE documentation portal for the FortiSASE administration guidance and the FortiManager documentation portal for FortiCloud registration, entitlement, and management integration details.

QUESTION NO: 4

Which information does FortiSASE use to bring network lockdown into effect on an endpoint?

A. Zero-day malware detection on endpoint

B. The number of critical vulnerabilities detected on the endpoint

C. The security posture of the endpoint based on ZTNA tags

D. The connection status of the tunnel to FortiSASE

ANSWER: C

Explanation:

FortiSASE uses the security posture of the endpoint based on ZTNA tags to determine whether network lockdown must be applied. ZTNA tags are endpoint posture labels supplied through FortiClient and FortiClient EMS. They represent evaluated device conditions, such as whether the endpoint meets an organization's required security and compliance state. FortiSASE can consume these tags as part of its endpoint-aware access-control and security enforcement workflow. When the endpoint posture changes so that it matches a condition configured for lockdown, FortiSASE can restrict the endpoint's network access according to the applicable lockdown policy. This provides dynamic enforcement: access decisions are tied to the device's current assessed state rather than relying solely on the user identity, a static connection state, or a one-time security event. Administrators therefore define the relevant posture conditions in EMS tags and use those tags in FortiSASE policy configuration to enforce the intended response. Fortinet documents endpoint posture and tag-based access control as core elements of its zero-trust access architecture. See the FortiSASE Administration Guide and the FortiClient EMS Administration Guide.

QUESTION NO: 5

Refer to the exhibits.

How will the application vulnerabilities be patched, based on the exhibits provided?

A. The vulnerability will be patched automatically based on the endpoint profile configuration.

B. The vulnerability will be patched by installing the patch from the vendor's website.

C. The end user will patch the vulnerabilities using the FortiClient software.

D. An administrator will patch the vulnerability remotely using FortiSASE.

ANSWER: B

Explanation:

The vulnerability will be patched by installing the patch from the vendor's website. FortiSASE endpoint posture and FortiClient vulnerability information are used to identify installed applications, their versions, and known vulnerabilities so that device compliance and risk can be assessed. When a vulnerable third-party application is identified, remediation consists of obtaining and applying the software publisher's update. The vendor is the authoritative source for the application installer, security update, prerequisites, and version-specific remediation instructions. Installing that update brings the affected application to a version in which the reported vulnerability has been addressed, allowing a subsequent endpoint assessment to reflect the corrected application state. FortiSASE integrates endpoint telemetry and security controls into its SASE service, while the application publisher remains responsible for issuing and distributing patches for its own products. See Fortinet's FortiSASE documentation for product and endpoint-security integration guidance, and the FortiClient documentation for endpoint feature documentation.

QUESTION NO: 6

Refer to the exhibits.

A FortiSASE administrator has configured an antivirus profile in the security profile group and applied it to the internet access policy. Remote users are still able to download the eicar.com-zip file from

Which configuration on FortiSASE is allowing users to perform the download?

A. Web filter is allowing the URL.

B. Deep inspection is not enabled.

C. Application control is exempting all the browser traffic.

D. Intrusion prevention is disabled.

ANSWER: B

Explanation:

Deep inspection is not enabled. The EICAR test archive is being downloaded through an encrypted HTTPS session, so FortiSASE must decrypt the session payload before the antivirus engine can examine the transferred ZIP file. When SSL inspection is configured as certificate inspection, FortiSASE validates and inspects TLS certificate and connection information but does not decrypt and scan the encrypted HTTP content. As a result, the antivirus profile attached through the security profile group cannot access the EICAR file's contents and cannot apply its malware-detection action to that download.

Enabling deep SSL inspection for the applicable internet-access traffic allows FortiSASE to perform TLS decryption, inspect the actual file payload, and then apply the antivirus profile to detect the EICAR signature and block the transfer according to the configured profile action. Clients must trust the FortiSASE SSL-inspection CA certificate so that browsers can establish the decrypted-and-re-encrypted TLS connection without certificate warnings. Fortinet describes the distinction between certificate inspection and deep inspection in its Deep inspection documentation and provides FortiSASE configuration guidance in the FortiSASE Administration Guide.

QUESTION NO: 7

An organization enables privacy protection for FortiSASE logs by hashing user-identifying information.

Which two operational outcomes does hashing provide? (Choose two.)

A. It obscures the original readable user-identifying information.

B. It preserves a consistent value for correlating related user activity.

C. It allows administrators to decrypt the original user identity when needed.

D. It prevents logs from being deleted when the retention period expires.

ANSWER: A B

Explanation:

Hashing prevents administrators from directly viewing the original readable user-identifying value in applicable log views. This helps protect user privacy while logs are reviewed and analyzed.

The same input produces a consistent derived value, allowing analysts to correlate activity associated with the same anonymized user across related log records. Hashing does not encrypt log data for later decryption, and it does not extend the configured FortiSASE log-retention period.