

FCSS_SASE_AD-25 Test Fee - Test FCSS_SASE_AD-25 Centres



BONUS!!! Download part of Pass4guide FCSS_SASE_AD-25 dumps for free: <https://drive.google.com/open?id=1v5V4QTYU2qQKiWIKpc8xB64p6w2NAjHE>

The Pass4guide are one of the high-in-demand and top-rated platforms that has been offering real, valid, and updated FCSS - FortiSASE 25 Administrator (FCSS_SASE_AD-25) practice test questions for many years. Over this long time period countless candidates have got success in their dream FCSS - FortiSASE 25 Administrator (FCSS_SASE_AD-25) certification exam. They all got help from FCSS - FortiSASE 25 Administrator (FCSS_SASE_AD-25) exam questions and easily crack the final Fortinet FCSS_SASE_AD-25 exam.

Fortinet FCSS_SASE_AD-25 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• SASE Architecture and Components: This section of the exam measures the skills of Network Engineers and introduces the fundamentals of SASE within enterprise environments. Candidates are expected to understand the SASE architecture, identify FortiSASE components, and build deployment cases for real-world scenarios. The content emphasizes how SASE can be integrated into a hybrid network, showcasing secure design principles and the use of FortiSASE capabilities to support business and security objectives.
Topic 2	<ul style="list-style-type: none">• SASE Deployment: This section of the exam measures the knowledge of Implementation Consultants and focuses on the practical aspects of deploying FortiSASE. Candidates will explore user onboarding methods, configuration of administration settings, and the application of security posture checks with compliance rules. The exam also includes key functions such as SIA, SSA, and SPA, alongside the design of security profiles that perform effective content inspection. By combining these tasks, learners demonstrate readiness to roll out secure and scalable deployments.

Topic 3	<ul style="list-style-type: none"> Advanced FortiSASE Solutions: This section of the exam measures the expertise of Solution Architects and validates the ability to work with advanced FortiSASE features. It covers deployment of SD-WAN using FortiSASE, implementation of Zero Trust Network Access (ZTNA), and the overall role of FortiSASE in optimizing enterprise connectivity. The section highlights how these advanced solutions improve flexibility, enforce zero-trust principles, and extend security controls across distributed networks and cloud systems.
Topic 4	<ul style="list-style-type: none"> Analytics and Monitoring: This section of the exam measures the skills of Security Analysts and emphasizes the monitoring and reporting aspects of FortiSASE. Candidates are expected to configure dashboards, logging settings, and analyze reports for user traffic and security issues. Additionally, they must use FortiSASE logs to identify potential threats and provide insights into incidents or abnormal behavior. The focus is on leveraging analytics for operational visibility and strengthening the organization's security posture.

>> FCSS_SASE_AD-25 Test Fee <<

Test FCSS_SASE_AD-25 Centres & Reliable Study FCSS_SASE_AD-25 Questions

Pass4guide provide you with the most authoritative and the fullest Fortinet FCSS_SASE_AD-25 Exam Dumps, thus the hit rate is very high. All questions that may appear in the exam are included in our exam dumps. With the changes of exam outline, we also update our exam dumps at any time. Pass4guide pdf real questions and answers can prevent you from wasting lots of time and efforts on preparing for the exam and can help you sail through you exam with ease and high efficiency. But even you fail the exam, we assure we will give you FULL REFUND. Opportunities always for those who are well prepared and we wish you not to miss the good opportunities.

Fortinet FCSS - FortiSASE 25 Administrator Sample Questions (Q24-Q29):

NEW QUESTION # 24

Which event log subtype captures FortiSASE SSL VPN user creation?

- A. Endpoint Events
- B. VPN Events
- C. Administrator Events
- D. User Events

Answer: D

Explanation:

The event log subtype that captures FortiSASE SSL VPN user creation is User Events . This subtype is specifically designed to log activities related to user management, such as creating, modifying, or deleting user accounts. When an SSL VPN user is created, it falls under this category because it involves adding a new user to the system.

Here's why the other options are incorrect:

A . Endpoint Events: These logs pertain to activities related to endpoint devices, such as device registration, compliance checks, or security posture assessments. SSL VPN user creation is unrelated to endpoint events.

B . VPN Events: These logs capture activities related to VPN connections, such as session establishment, termination, or errors. While SSL VPN usage generates VPN events, the creation of a user account itself is not logged under this subtype.

D . Administrator Events: These logs track actions performed by administrators, such as configuration changes or policy updates. While an administrator might create the SSL VPN user, the specific event of user creation is categorized under User Events, not Administrator Events.

Fortinet FCSS FortiSASE Documentation - Event Logging and Subtypes

FortiSASE Administration Guide - Monitoring and Logging

NEW QUESTION # 25

Refer to the exhibit.

The daily report for application usage for internet traffic shows an unusually high number of unknown applications by category.

What are two possible explanations for this? (Choose two.)

- A. The inline-CASB application control profile does not have application categories set to Monitor.
- B. Deep inspection is not being used to scan traffic.
- C. The private access policy must be set to log Security Events.
- D. Certificate inspection is not being used to scan application traffic.

Answer: B,D

NEW QUESTION # 26

Refer to the exhibit.

□ The daily report for application usage for internet traffic shows an unusually high number of unknown applications by category. What are two possible explanations for this? (Choose two.)

- A. The inline-CASB application control profile does not have application categories set to Monitor.
- B. Deep inspection is not being used to scan traffic.
- C. The private access policy must be set to log Security Events.
- D. Certificate inspection is not being used to scan application traffic.

Answer: A,B

NEW QUESTION # 27

When viewing the daily summary report generated by FortiSASE, the administrator notices that the report contains very little data. What is a possible explanation for this almost empty report?

- A. Digital experience monitoring is not configured.
- B. There are no security profile groups applied to all policies.
- C. The web filter security profile is not set to Monitor.
- D. Log allowed traffic is set to Security Events for all policies.

Answer: D

Explanation:

The issue of an almost empty daily summary report in FortiSASE can often be traced back to how logging is configured within the system. Specifically, if "Log Allowed Traffic" is set to "Security Events" for all policies, it means that only security-related events (such as threats or anomalies) are being logged, while normal, allowed traffic is not being recorded. Since most traffic in a typical network environment is allowed, this configuration would result in very little data being captured and subsequently reported in the daily summary.

Here's a breakdown of why the other options are less likely to be the cause:

- B . There are no security profile groups applied to all policies: While applying security profiles is important for comprehensive protection, their absence does not directly affect the volume of data in reports unless specific logging settings are also misconfigured.
- C . The web filter security profile is not set to Monitor: This option pertains specifically to web filtering activities. Even if web filtering is not set to monitor mode, other types of traffic and logs should still populate the report.
- D . Digital experience monitoring is not configured: Digital Experience Monitoring (DEM) focuses on user experience metrics rather than general traffic logging. Its absence would not lead to an almost empty report.

To resolve this issue, administrators should review the logging settings across all policies and ensure that "Log Allowed Traffic" is appropriately configured to capture the necessary data for reporting purposes.

Fortinet FCSS FortiSASE Documentation - Reporting and Logging Best Practices FortiSASE Administration Guide - Configuring Logging Settings

NEW QUESTION # 28

Refer to the exhibit.

□ The daily report for application usage shows an unusually high number of unknown applications by category. What are two possible explanations for this? (Choose two.)

- A. The inline-CASB application control profile does not have application categories set to Monitor
- B. Zero trust network access (ZTNA) tags are not being used to tag the correct users.

- Answer: A,C**

• • • • •

Test FCSS_SASE_AD-25 Centres: https://www.pass4guide.com/FCSS_SASE_AD-25-exam-guide-torrent.html

- P.S. Free & New FCSS SASE AD-25 dumps are available on Google Drive shared by Pass4guide:

<https://drive.google.com/open?id=1v5V4QTYU2qQKiWiKpc8xB64p6w2NAjHE>