# Fortinet

## Exam Questions FCSS_SASE_AD-24

FCSS - FortiSASE 24 Administrator

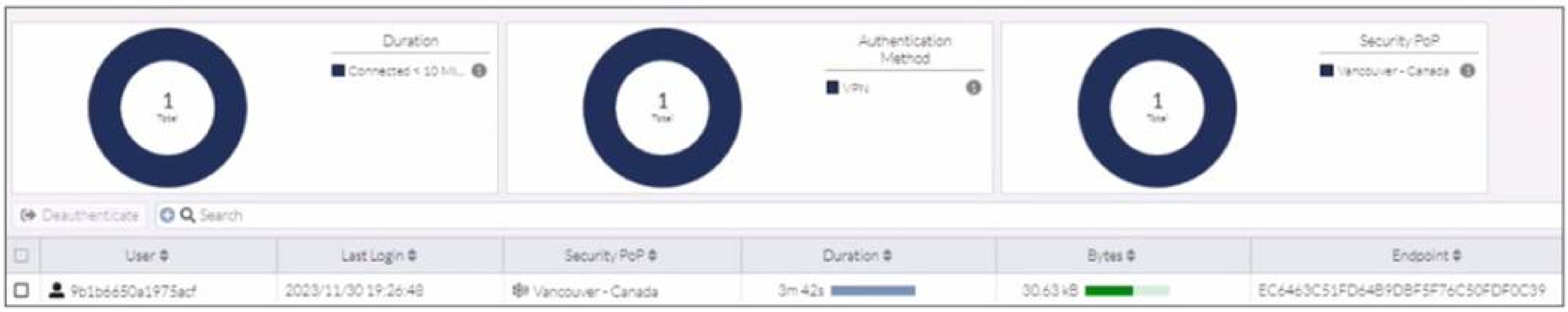
**NEW QUESTION 1**
A FortiSASE administrator is configuring a Secure Private Access (SPA) solution to share endpoint information with a corporate FortiGate.
Which three configuration actions will achieve this solution? (Choose three.)

A. Add the FortiGate IP address in the secure private access configuration on FortiSASE.
B. Use the FortiClient EMS cloud connector on the corporate FortiGate to connect to FortiSASE
C. Register FortiGate and FortiSASE under the same FortiCloud account.
D. Authorize the corporate FortiGate on FortiSASE as a ZTNA access proxy.
E. Apply the FortiSASE zero trust network access (ZTNA) license on the corporate FortiGate.

**Answer:** BCD

**Explanation:**
References:
? FortiOS 7.2 Administration Guide: Provides details on configuring Secure Private Access and integrating with FortiGate.
? FortiSASE 23.2 Documentation: Explains how to set up and manage connections between FortiSASE and corporate FortiGate.

**NEW QUESTION 2**
Refer to the exhibit.



| □ | User ⇕ | Last Login ⇕ | Security PoP ⇕ | Duration ⇕ | Bytes ⇕ | Endpoint ⇕ |
|---|---|---|---|---|---|---|
| □ | 9b1b6650a1975acf | 2023/11/30 19:26:48 | Vancouver - Canada | 3m 42s | 30.63 kB | EC6463C51FD64B9DBF5F76C50FDF0C39 |

In the user connection monitor, the FortiSASE administrator notices the user name is showing random characters. Which configuration change must the administrator make to get proper user information?

A. Turn off log anonymization on FortiSASE.
B. Add more endpoint licenses on FortiSASE.
C. Configure the username using FortiSASE naming convention.
D. Change the deployment type from SWG to VPN.

**Answer:** A

**Explanation:**
In the user connection monitor, the random characters shown for the username indicate that log anonymization is enabled. Log anonymization is a feature that hides the actual user informationin the logs for privacy and security reasons. To display proper user information, you need to disable log anonymization.
? Log Anonymization:
? Disabling Log Anonymization:
References:
? FortiSASE 23.2 Documentation: Provides detailed steps on enabling and disabling log anonymization.
? Fortinet Knowledge Base: Explains the impact of log anonymization on user monitoring and logging.

**NEW QUESTION 3**
Which secure internet access (SIA) use case minimizes individual endpoint configuration?

A. Site-based remote user internet access
B. Agentless remote user internet access
C. SIA for SSL VPN remote users
D. SIA using ZTNA

**Answer:** B

**Explanation:**
Theagentless remote user internet accessuse case is designed to minimize individual endpoint configuration. In this scenario, FortiSASE provides secure internet access without requiring the installation of an agent on the endpoint device. This approach is particularly useful for environments with unmanaged devices or temporary users, as it eliminates the need for complex configurations on each endpoint. Instead, security policies are enforced at the network level, ensuring consistent protection without relying on endpoint-specific software.
Here??s why the other options are incorrect:
? A. Site-based remote user internet access:This use case involves securing internet access for users at a specific site or location, typically through a gateway or firewall. While it simplifies configuration for all users at that site, it does not specifically minimize individual endpoint configuration for remote users.
? C. SIA for SSL VPN remote users:SSL VPN requires users to connect to the corporate network via a client or browser-based interface. This approach often involves additional configuration on the endpoint, such as installing and configuring the SSL VPN client.
? D. SIA using ZTNA:Zero Trust Network Access (ZTNA) focuses on verifying the identity and posture of devices before granting access to resources. While ZTNA enhances security, it may require endpoint agents or posture checks, which involve some level of endpoint configuration.
References:
? Fortinet FCSS FortiSASE Documentation - Secure Internet Access (SIA) Use Cases
? FortiSASE Administration Guide - Agentless Remote User Access

**NEW QUESTION 4**
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 when viewing and analyzing logs by hashing data using salt. This approach ensures that sensitive user information is obfuscated, enhancing privacy and security.
? Hashing Data with Salt:
? Security and Privacy:
References:
? FortiOS 7.2 Administration Guide: Provides information on log management and data protection techniques.
? FortiSASE 23.2 Documentation: Details on how FortiSASE implements data hashing and salting to secure user information in logs.

**NEW QUESTION 5**
Which role does FortiSASE play in supporting zero trust network access (ZTNA) principles9

A. It offers hardware-based firewalls for network segmentation.
B. It integrates with software-defined network (SDN) solutions.
C. It can identify attributes on the endpoint for security posture check.
D. It enables VPN connections for remote employees.

**Answer:** C

**Explanation:**
FortiSASE supports zero trust network access (ZTNA) principles by identifying attributes on the endpoint for security posture checks. ZTNA principles require continuous verification of user and device credentials, as well as their security posture, before granting access to network resources.
? Security Posture Check:
? Zero Trust Network Access (ZTNA):
References:
? FortiOS 7.2 Administration Guide: Provides information on ZTNA and endpoint security posture checks.
? FortiSASE 23.2 Documentation: Details on how FortiSASE implements ZTNA principles.

**NEW QUESTION 6**
An organization must block user attempts to log in to non-company resources while using Microsoft Office 365 to prevent users from accessing unapproved cloud resources.
Which FortiSASE feature can you implement to achieve this requirement?

A. Web Filter with Inline-CASB
B. SSL deep inspection
C. Data loss prevention (DLP)
D. Application Control with Inline-CASB

**Answer:** A

**Explanation:**
To block user attempts to log in to non-company resources while using Microsoft Office 365, theWeb Filter with Inline-CASBfeature in FortiSASE is the most appropriate solution. Inline-CASB (Cloud Access Security Broker) provides real-time visibility and control over cloud application usage. When combined with Web Filtering, it can enforce policies to restrict access to unauthorized or non-company resources within sanctioned applications like Microsoft Office 365. This ensures that users cannot access unapproved cloud resources while still allowing legitimate use of Office 365.
Here??s why the other options are incorrect:
? B. SSL deep inspection:While SSL deep inspection is useful for decrypting and inspecting encrypted traffic, it does not specifically address the need to block access to non-companyresources within Office 365. It focuses on securing traffic rather than enforcing application-specific policies.
? C. Data loss prevention (DLP):DLP is designed to prevent sensitive data from being leaked or exfiltrated. While it is a valuable security feature, it does not directly block access to non-company resources within Office 365.
? D. Application Control with Inline-CASB:Application Control focuses on managing access to specific applications rather than enforcing granular policies within an application like Office 365. Web Filter with Inline-CASB is better suited for this use case.
References:
? Fortinet FCSS FortiSASE Documentation - Inline-CASB and Web Filtering
? FortiSASE Administration Guide - Securing Cloud Applications
================

**NEW QUESTION 7**
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. Log allowed traffic is set to Security Events for all policies.
B. There are no security profile groups applied to all policies.
C. The web filter security profile is not set to Monitor.
D. Digital experience monitoring is not configured.

**Answer:** A

**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.
References:
? Fortinet FCSS FortiSASE Documentation - Reporting and Logging Best Practices
? FortiSASE Administration Guide - Configuring Logging Settings

**NEW QUESTION 8**
Which event log subtype captures FortiSASE SSL VPN user creation?

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

**Answer:** C

**Explanation:**
Theevent log subtypethat 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.
References:
? Fortinet FCSS FortiSASE Documentation - Event Logging and Subtypes
? FortiSASE Administration Guide - Monitoring and Logging

**NEW QUESTION 9**
Which statement describes the FortiGuard forensics analysis feature on FortiSASE?

A. It can help troubleshoot user-to-application performance issues.
B. It can help customers identify and mitigate potential risks to their network.
C. It can monitor endpoint resources in real-time.
D. It is a 24x7x365 monitoring service of your FortiSASE environment.

**Answer:** B

**Explanation:**
TheFortiGuard forensics analysis featureon FortiSASE is designed to help customersidentify and mitigate potential risks to their network. This feature provides detailed insights into suspicious activities, threats, and anomalies detected by FortiSASE. By analyzing logs, traffic patterns, and threat intelligence, FortiGuard forensics enables administrators to investigate incidents, understand their root causes, and take proactive measures to secure the network.
Here??s why the other options are incorrect:
? A. It can help troubleshoot user-to-application performance issues:Performance troubleshooting is typically handled by features like Digital Experience Monitoring (DEM) or application performance monitoring tools, not forensics analysis.
? C. It can monitor endpoint resources in real-time:Real-time endpoint monitoring is a function of endpoint security solutions like FortiClient or FortiEDR, not FortiGuard forensics analysis.
? D. It is a 24x7x365 monitoring service of your FortiSASE environment:While Fortinet offers managed services for continuous monitoring, FortiGuard forensics analysis is not a dedicated monitoring service. Instead, it focuses on post-incident investigation and risk mitigation.
References:
? Fortinet FCSS FortiSASE Documentation - FortiGuard Forensics Analysis
? FortiSASE Administration Guide - Threat Detection and Response

**NEW QUESTION 10**
What are two requirements to enable the MSSP feature on FortiSASE? (Choose two.)

A. Add FortiCloud premium subscription on the root FortiCloud account.
B. Configure MSSP user accounts and permissions on the FortiSASE portal.
C. Assign role-based access control (RBAC) to IAM users using FortiCloud IAM portal.
D. Enable multi-tenancy on the FortiSASE portal.

**Answer:** CD

**Explanation:**
To enable theMSSP (Managed Security Service Provider)feature on FortiSASE, two key requirements must be met:
? Assign role-based access control (RBAC) to IAM users using FortiCloud IAM
portal (Option C):RBAC is essential for managing permissions and ensuring that different customers (tenants) have appropriate access levels. The FortiCloud Identity and Access Management (IAM) portal allows administrators to define roles and assign them to users, ensuring secure and granular control over resources.
? Enable multi-tenancy on the FortiSASE portal (Option D):Multi-tenancy is a critical
feature for MSSPs, as it allows them to manage multiple customer environments (tenants) from a single FortiSASE instance. Each tenant operates independently

with its own configurations, policies, and reporting, while the MSSP retains centralized control.
Here??s why the other options are incorrect:
? A. Add FortiCloud premium subscription on the root FortiCloud account:While FortiCloud subscriptions may enhance functionality, they are not specifically required to enable the MSSP feature.
? B. Configure MSSP user accounts and permissions on the FortiSASE portal:User accounts and permissions are managed through the FortiCloud IAM portal, not directly on the FortiSASE portal.
References:
? Fortinet FCSS FortiSASE Documentation - MSSP Feature Configuration
? FortiSASE Administration Guide - Multi-Tenancy and RBAC Setup

**NEW QUESTION 10**
In which three ways does FortiSASE help organizations ensure secure access for remote workers? (Choose three.)

A. It enforces multi-factor authentication (MFA) to validate remote users.
B. It secures traffic from endpoints to cloud applications.
C. It uses the identity & access management (IAM) portal to validate the identities of remote workers.
D. It offers zero trust network access (ZTNA) capabilities.
E. It enforces granular access policies based on user identities.

**Answer:** BDE

**Explanation:**
FortiSASE provides several features to ensure secure access for remote workers. The following three ways are particularly relevant:
? It secures traffic from endpoints to cloud applications (Option B):FortiSASE
secures all traffic between remote endpoints and cloud applications by inspecting it in real time. This includes applying security policies, threat detection, and data protection measures to ensure that traffic is safe and compliant.
? It offers zero trust network access (ZTNA) capabilities (Option D):ZTNA ensures
that remote workers are granted access to resources based on strict verification of their identity and device posture. By treating all users and devices as untrusted by default, ZTNA minimizes the risk of unauthorized access and lateral movement within the network.
? It enforces granular access policies based on user identities (Option E):FortiSASE
allows administrators to define and enforce fine-grained access policies based on user identities, roles, and other attributes. This ensures that remote workers only have access to the resources they need, reducing the attack surface.
Here??s why the other options are incorrect:
? A. It enforces multi-factor authentication (MFA) to validate remote users:While MFA is a critical security measure, it is typically implemented through identity providers (e.g., FortiAuthenticator or third-party solutions) rather than directly through FortiSASE.
? C. It uses the identity & access management (IAM) portal to validate the identities of remote workers:FortiSASE integrates with IAM systems but does not use the IAM portal itself to validate identities. Identity validation is handled through authentication mechanisms like SAML, LDAP, or OAuth.
References:
? Fortinet FCSS FortiSASE Documentation - Secure Remote Access
? FortiSASE Administration Guide - ZTNA and Access Policies

**NEW QUESTION 11**
What are two advantages of using zero-trust tags? (Choose two.)

A. Zero-trust tags can be used to allow or deny access to network resources
B. Zero-trust tags can determine the security posture of an endpoint.
C. Zero-trust tags can be used to create multiple endpoint profiles which can be applied to different endpoints
D. Zero-trust tags can be used to allow secure web gateway (SWG) access

**Answer:** AB

**Explanation:**
Zero-trust tags are critical in implementing zero-trust network access (ZTNA) policies. Here are the two key advantages of using zero-trust tags:
? Access Control (Allow or Deny):
? Determining Security Posture:
References:
? FortiOS 7.2 Administration Guide: Provides detailed information on configuring and using zero-trust tags for access control and security posture assessment.
? FortiSASE 23.2 Documentation: Explains how zero-trust tags are implemented and used within the FortiSASE environment for enhancing security and compliance.

**NEW QUESTION 15**
Which statement best describes the Digital Experience Monitor (DEM) feature on FortiSASE?

A. It provides end-to-end network visibility from all the FortiSASE security PoPs to a specific SaaS application.
B. It can be used to request a detailed analysis of the endpoint from the FortiGuard team.
C. It requires a separate DEM agent to be downloaded from the FortiSASE portal and installed on the endpoint.
D. It can help IT and security teams ensure consistent security monitoring for remote users.

**Answer:** A

**Explanation:**
TheDigital Experience Monitor (DEM)feature in FortiSASE is designed to provideend-to-end network visibilityby monitoring the performance and health of connections between FortiSASE security Points of Presence (PoPs) and specific SaaS applications. This ensures that administrators can identify and troubleshoot issues related to latency, jitter, packet loss, and other network performance metrics that could impact user experience when accessing cloud-based services.
Here??s why the other options are incorrect:
? B. It can be used to request a detailed analysis of the endpoint from the FortiGuard team:This is incorrect because DEM focuses on network performance monitoring, not endpoint analysis. Endpoint analysis would typically involve tools like FortiClient or FortiEDR, not DEM.
? C. It requires a separate DEM agent to be downloaded from the FortiSASE portal and installed on the endpoint:This is incorrect because DEM operates at the network level and does not require an additional agent to be installed on endpoints.
? D. It can help IT and security teams ensure consistent security monitoring for remote users:While DEM indirectly supports security by ensuring optimal network

performance, its primary purpose is to monitor and improve the digital experience rather than enforce security policies.
References:
? Fortinet FCSS FortiSASE Documentation - Digital Experience Monitoring Overview
? FortiSASE Administration Guide - Configuring DEM
================

**NEW QUESTION 19**
......