



# Fortinet

## Exam Questions FCSS\_SASE\_AD-24

FCSS - FortiSASE 24 Administrator

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

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. Log allowed traffic is set to Security Events for all policies.
- C. The web filter security profile is not set to Monitor
- D. There are no security profile group applied to all policies.

**Answer: B**

#### Explanation:

If the daily summary report generated by FortiSASE contains very little data, one possible explanation is that the "Log allowed traffic" setting is configured to log only "Security Events" for all policies. This configuration limits the amount of data logged, as it only includes security events and excludes normal allowed traffic.

? Log Allowed Traffic Setting:

? Impact on Report Data:

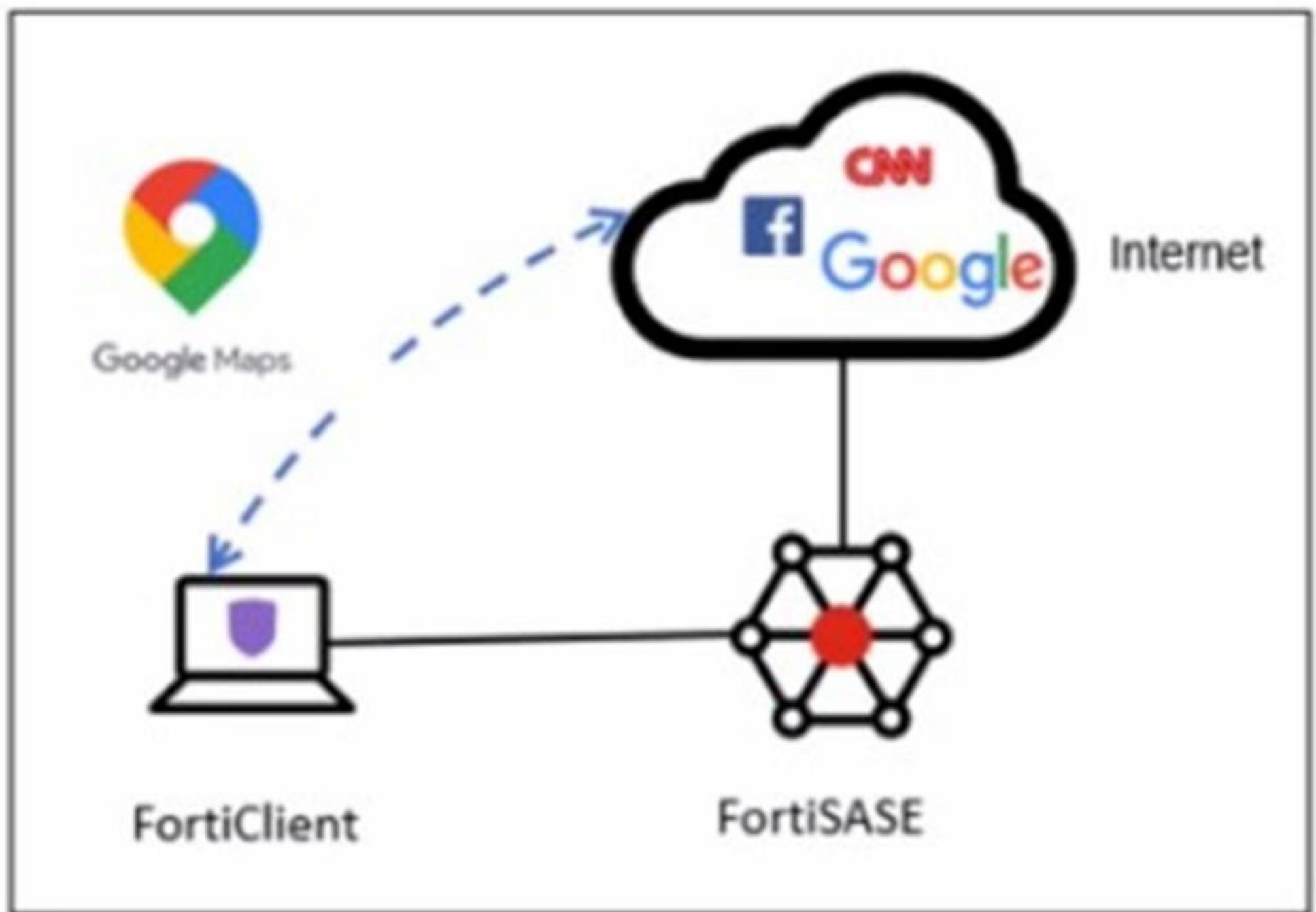
References:

? FortiOS 7.2 Administration Guide: Provides details on configuring logging settings for traffic policies.

? FortiSASE 23.2 Documentation: Explains the impact of logging configurations on report generation and data visibility.

### NEW QUESTION 2

Refer to the exhibit.



A company has a requirement to inspect all the endpoint internet traffic on FortiSASE, and exclude Google Maps traffic from the FortiSASE VPN tunnel and redirect it to the endpoint physical interface.

Which configuration must you apply to achieve this requirement?

- A. Exempt the Google Maps FQDN from the endpoint system proxy settings.
- B. Configure a static route with the Google Maps FQDN on the endpoint to redirect traffic
- C. Configure the Google Maps FQDN as a split tunneling destination on the FortiSASE endpoint profile.
- D. Change the default DNS server configuration on FortiSASE to use the endpoint system DNS.

**Answer: C**

#### Explanation:

To meet the requirement of inspecting all endpoint internet traffic on FortiSASE while excluding Google Maps traffic from the FortiSASE VPN tunnel and redirecting it to the endpoint's physical interface, you should configure split tunneling. Split tunneling allows specific traffic to bypass the VPN tunnel and be routed directly through the endpoint's local interface.

? Split Tunneling Configuration:

? Implementation Steps:

References:

- ? FortiOS 7.2 Administration Guide: Provides details on split tunneling configuration.
- ? FortiSASE 23.2 Documentation: Explains how to set up and manage split tunneling for specific destinations.

**NEW QUESTION 3**

A customer needs to implement device posture checks for their remote endpoints while accessing the protected server. They also want the TCP traffic between the remote endpoints and the protected servers to be processed by FortiGate.  
In this scenario, which three setups will achieve the above requirements? (Choose three.)

- A. Configure ZTNA tags on FortiGate.
- B. Configure FortiGate as a zero trust network access (ZTNA) access proxy.
- C. Configure ZTNA servers and ZTNA policies on FortiGate.
- D. Configure private access policies on FortiSASE with ZTNA.
- E. Sync ZTNA tags from FortiSASE to FortiGate.

**Answer:** ABC

**Explanation:**

To meet the requirements of implementing device posture checks for remote endpoints and ensuring that TCP traffic between the endpoints and protected servers is processed by FortiGate, the following three setups are necessary:

? Configure ZTNA tags on FortiGate (Option A): ZTNA (Zero Trust Network Access) tags are used to define access control policies based on the security posture of devices. By configuring ZTNA tags on FortiGate, administrators can enforce granular access controls, ensuring that only compliant devices can access protected resources.

? Configure FortiGate as a zero trust network access (ZTNA) access proxy (Option B): FortiGate can act as a ZTNA access proxy, which allows it to mediate and secure connections between remote endpoints and protected servers. This setup ensures that all TCP traffic passes through FortiGate, enabling inspection and enforcement of security policies.

? Configure ZTNA servers and ZTNA policies on FortiGate (Option C): To enable ZTNA functionality, administrators must define ZTNA servers (the protected resources) and create ZTNA policies on FortiGate. These policies determine how traffic is routed, inspected, and controlled based on device posture and user identity.

Here's why the other options are incorrect:

? D. Configure private access policies on FortiSASE with ZTNA: While FortiSASE supports ZTNA, the requirement specifies that TCP traffic must be processed by FortiGate. Configuring private access policies on FortiSASE would route traffic through FortiSASE instead of FortiGate, which does not meet the stated requirements.

? E. Sync ZTNA tags from FortiSASE to FortiGate: Synchronizing ZTNA tags is unnecessary in this scenario because the focus is on FortiGate processing the traffic. The tags can be directly configured on FortiGate without involving FortiSASE.

References:

- ? Fortinet FCSS FortiSASE Documentation - Zero Trust Network Access (ZTNA) Deployment
- ? FortiGate Administration Guide - ZTNA Configuration

=====

**NEW QUESTION 4**

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, the Web Filter with Inline-CASB feature 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-company resources 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 5**

Which two deployment methods are used to connect a FortiExtender as a FortiSASE LAN extension? (Choose two.)

- A. Connect FortiExtender to FortiSASE using FortiZTP
- B. Enable Control and Provisioning Wireless Access Points (CAPWAP) access on the FortiSASE portal.
- C. Enter the FortiSASE domain name in the FortiExtender GUI as a static discovery server
- D. Configure an IPsec tunnel on FortiSASE to connect to FortiExtender.

**Answer:** AC

**Explanation:**

There are two deployment methods used to connect a FortiExtender as a FortiSASE LAN extension:

? Connect FortiExtender to FortiSASE using FortiZTP:

? Enter the FortiSASE domain name in the FortiExtender GUI as a static discovery server:

References:

? FortiOS 7.2 Administration Guide: Details on FortiExtender deployment methods and configurations.

? FortiSASE 23.2 Documentation: Explains how to connect and configure FortiExtender with FortiSASE using FortiZTP and static discovery.

#### NEW QUESTION 6

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:

When configuring FortiSASE Secure Private Access (SPA) with SD-WAN integration, establishing a routing adjacency between FortiSASE and the FortiGate SD-WAN hub requires the use of the Border Gateway Protocol (BGP).

? BGP (Border Gateway Protocol):

? Routing Adjacency:

References:

? FortiOS 7.2 Administration Guide: Provides information on configuring BGP for SD-WAN integration.

? FortiSASE 23.2 Documentation: Details on setting up routing adjacencies using BGP for Secure Private Access with SD-WAN.

#### NEW QUESTION 7

To complete their day-to-day operations, remote users require access to a TCP-based application that is hosted on a private web server. Which FortiSASE deployment use case provides the most efficient and secure method for meeting the remote users' requirements?

- A. SD-WAN private access
- B. inline-CASB
- C. zero trust network access (ZTNA) private access
- D. next generation firewall (NGFW)

**Answer:** C

#### Explanation:

Zero Trust Network Access (ZTNA) private access provides the most efficient and secure method for remote users to access a TCP-based application hosted on a private web server. ZTNA ensures that only authenticated and authorized users can access specific applications based on predefined policies, enhancing security and access control.

? Zero Trust Network Access (ZTNA):

? Secure and Efficient Access:

References:

? FortiOS 7.2 Administration Guide: Provides detailed information on ZTNA and its deployment use cases.

? FortiSASE 23.2 Documentation: Explains how ZTNA can be used to provide secure access to private applications for remote users.

#### NEW QUESTION 8

Refer to the exhibit.

## Security Logs

Log Details

Destination

Destination IP

151.101.40.81


Destination Port

443

Destination Country/Region

United States

Traffic Type

 Internet Access

Destination UUID

4a501662-f85f-51ed-5194-7e45b3d369cd

Hostname

www.bbc.com


URL

https://www.bbc.com/

Application Control

Action

Action

 Blocked

Threat

16,777,216

Policy ID

8

Policy UUID

7d56f000-b41e-51ee-f96b-d0b4d9fb3c2b


Policy Type

policy

Security

Web Filter

Profile Group

 SIA (Internet Access)

Request Type

direct

Direction

incoming

Banned Word

fight

Message

URL was blocked because it contained banned word(s).

To allow access, which web tiller configuration must you change on FortiSASE?

- A. FortiGuard category-based filter
- B. content filter
- C. URL Filter
- D. inline cloud access security broker (CASB) headers

**Answer:** B

#### NEW QUESTION 9

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 10

Which FortiSASE feature ensures least-privileged user access to all applications?

- A. secure web gateway (SWG)
- B. SD-WAN
- C. zero trust network access (ZTNA)
- D. thin branch SASE extension

**Answer:** C

#### Explanation:

Zero Trust Network Access (ZTNA) is the FortiSASE feature that ensures least-privileged user access to all applications. ZTNA operates on the principle of "never trust, always verify," providing secure access based on the identity of users and devices, regardless of their location.

? Zero Trust Network Access (ZTNA):

? Implementation:

References:

? FortiOS 7.2 Administration Guide: Provides detailed information on ZTNA and its role in ensuring least-privileged access.

? FortiSASE 23.2 Documentation: Explains the implementation and benefits of ZTNA within the FortiSASE environment.

#### NEW QUESTION 10

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:

The Digital Experience Monitor (DEM) feature in FortiSASE is designed to provide end-to-end network visibility by 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 15

Refer to the exhibit.

## Daily report for application usage



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. Certificate inspection is not being used to scan application traffic.
- B. The inline-CASB application control profile does not have application categories set to Monitor
- C. Zero trust network access (ZTNA) tags are not being used to tag the correct users.
- D. Deep inspection is not being used to scan traffic.

**Answer:** BD

### NEW QUESTION 16

Which statement applies to a single sign-on (SSO) deployment on FortiSASE?

- A. SSO overrides any other previously configured user authentication.
- B. SSO identity providers can be integrated using public and private access types.
- C. SSO is recommended only for agent-based deployments.
- D. SSO users can be imported into FortiSASE and added to user groups.

**Answer:** D

**Explanation:**

In aSingle Sign-On (SSO)deployment on FortiSASE,SSO users can be imported into FortiSASE and added to user groups. This allows administrators to manage SSO users within FortiSASE, enabling them to apply policies, permissions, and group-based access controls. By integrating SSO with FortiSASE, organizations can streamline user authentication and simplify access management while maintaining security. Here??s why the other options are incorrect:

? A. SSO overrides any other previously configured user authentication:This is incorrect because SSO does not automatically override other authentication methods. FortiSASE supports multiple authentication mechanisms, and SSO is just one of them. Administrators can configure fallback authentication methods if needed.

? B. SSO identity providers can be integrated using public and private access

types:While FortiSASE supports integration with various identity providers (e.g., SAML, LDAP, OAuth), the concept of "public and private access types" is not applicable to SSO configurations.

? C. SSO is recommended only for agent-based deployments:This is incorrect

because SSO can be used in both agent-based and agentless deployments. It is not limited to environments where agents are installed.

References:

? Fortinet FCSS FortiSASE Documentation - Single Sign-On (SSO) Integration

? FortiSASE Administration Guide - User Authentication and SSO

=====

**NEW QUESTION 21**

.....

## Relate Links

**100% Pass Your FCSS\_SASE\_AD-24 Exam with Examible Prep Materials**

[https://www.examible.com/FCSS\\_SASE\\_AD-24-exam/](https://www.examible.com/FCSS_SASE_AD-24-exam/)

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.examible.com/>