

Fortinet

Exam Questions FCSS_SASE_AD-23

FCSS FortiSASE 23 Administrator



NEW QUESTION 1

A customer wants to upgrade their legacy on-premises proxy to a cloud-based proxy for a hybrid network. Which FortiSASE features would help the customer to achieve this outcome?

- A. SD-WAN and NGFW
- B. SD-WAN and inline-CASB
- C. zero trust network access (ZTNA) and next generation firewall (NGFW)
- D. secure web gateway (SWG) and inline-CASB

Answer: D

Explanation:

For a customer looking to upgrade their legacy on-premises proxy to a cloud-based proxy for a hybrid network, the combination of Secure Web Gateway (SWG) and Inline Cloud Access Security Broker (CASB) features in FortiSASE will provide the necessary capabilities.

? Secure Web Gateway (SWG):

? Inline Cloud Access Security Broker (CASB):

References:

? FortiOS 7.2 Administration Guide: Details on SWG and CASB features.

? FortiSASE 23.2 Documentation: Explains how SWG and inline-CASB are used in cloud-based proxy solutions.

NEW QUESTION 2

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 3

You are designing a new network for Company X and one of the new cybersecurity policy requirements is that all remote user endpoints must always be connected and protected. Which FortiSASE component facilitates this always-on security measure?

- A. site-based deployment
- B. thin-branch SASE extension
- C. unified FortiClient
- D. inline-CASB

Answer: C

Explanation:

The unified FortiClient component of FortiSASE facilitates the always-on security measure required for ensuring that all remote user endpoints are always connected and protected.

? Unified FortiClient:

? Always-On Security:

References:

? FortiOS 7.2 Administration Guide: Provides information on configuring and managing FortiClient for endpoint security.

? FortiSASE 23.2 Documentation: Explains how FortiClient integrates with FortiSASE to deliver always-on security for remote endpoints.

NEW QUESTION 4

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 5

Which two additional components does FortiSASE use for application control to act as an inline-CASB? (Choose two.)

- A. intrusion prevention system (IPS)
- B. SSL deep inspection
- C. DNS filter
- D. Web filter with inline-CASB

Answer: BD

Explanation:

FortiSASE uses the following components for application control to act as an inline-CASB (Cloud Access Security Broker):

? SSL Deep Inspection:

? Web Filter with Inline-CASB:

References:

? FortiOS 7.2 Administration Guide: Details on SSL deep inspection and web filtering configurations.

? FortiSASE 23.2 Documentation: Explains how FortiSASE acts as an inline-CASB using SSL deep inspection and web filtering.

NEW QUESTION 6

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 7

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 8

When deploying FortiSASE agent-based clients, which three features are available compared to an agentless solution? (Choose three.)

- A. Vulnerability scan
- B. SSL inspection
- C. Anti-ransomware protection
- D. Web filter
- E. ZTNA tags

Answer: ABD

Explanation:

When deploying FortiSASE agent-based clients, several features are available that are not typically available with an agentless solution. These features enhance the security and management capabilities for endpoints.

? Vulnerability Scan:

? SSL Inspection:

? Web Filter:

References:

? FortiOS 7.2 Administration Guide: Explains the features and benefits of deploying agent-based clients.

? FortiSASE 23.2 Documentation: Details the differences between agent-based and agentless solutions and the additional features provided by agent-based deployments.

Secure Internet Access policy

Name ⓘ

Web Traffic

Source Scope

AllVPN UsersEdge Device

Source

All TrafficSpecify

User

All VPN UsersSpecify

👤 VPN_Users

×

+

Destination

All Internet TrafficSpecify

Service

🖥️ ALL

×

+

Profile Group

DefaultSpecify

SIA

Force Certificate Inspection ⓘ

🔵

Action

✓ Accept

🚫 Deny

Status

🟢 Enable

🔴 Disable

Logging Options

Log Allowed Traffic

🔵

Security Events

All Sessions

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 <https://eicar.org>. Traffic logs show traffic is allowed by the policy. Which configuration on FortiSASE is allowing users to perform the download?

- A. Web filter is allowing the traffic.
- B. IPS is disabled in the security profile group.
- C. The HTTPS protocol is not enabled in the antivirus profile.
- D. Force certificate inspection is enabled in the policy.

Answer: A

Explanation:

- ? Web Filtering Logs Analysis:
- ? Security Profile Group Configuration:
- ? Antivirus Profile Configuration:
- ? Policy Configuration:
- References:
- ? FortiGate Security 7.2 Study Guide: Provides details on the precedence of web filtering over antivirus in security profiles.
- ? Fortinet Knowledge Base: Detailed explanation of web filtering and antivirus profiles interaction.

NEW QUESTION 10

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 filter 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: C

Explanation:

The exhibit indicates that the URL <https://www.bbc.com> is being blocked due to containing a banned word ("fight"). To allow access to this specific URL, you need to adjust the URL filter settings on FortiSASE.

? URL Filtering:

? Modifying URL Filter:

References:

? FortiOS 7.2 Administration Guide: Provides details on configuring and managing URL filters.

? FortiSASE 23.2 Documentation: Explains how to set up and modify web filtering policies, including URL filters.

NEW QUESTION 10

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 12

Which role does FortiSASE play in supporting zero trust network access (ZTNA) principles?

- 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 14

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCSS_SASE_AD-23 Practice Exam Features:

- * FCSS_SASE_AD-23 Questions and Answers Updated Frequently
- * FCSS_SASE_AD-23 Practice Questions Verified by Expert Senior Certified Staff
- * FCSS_SASE_AD-23 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCSS_SASE_AD-23 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_SASE_AD-23 Practice Test Here](#)