



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

During FortiSASE provisioning, how many security points of presence (POPs) need to be configured by the FortiSASE administrator?

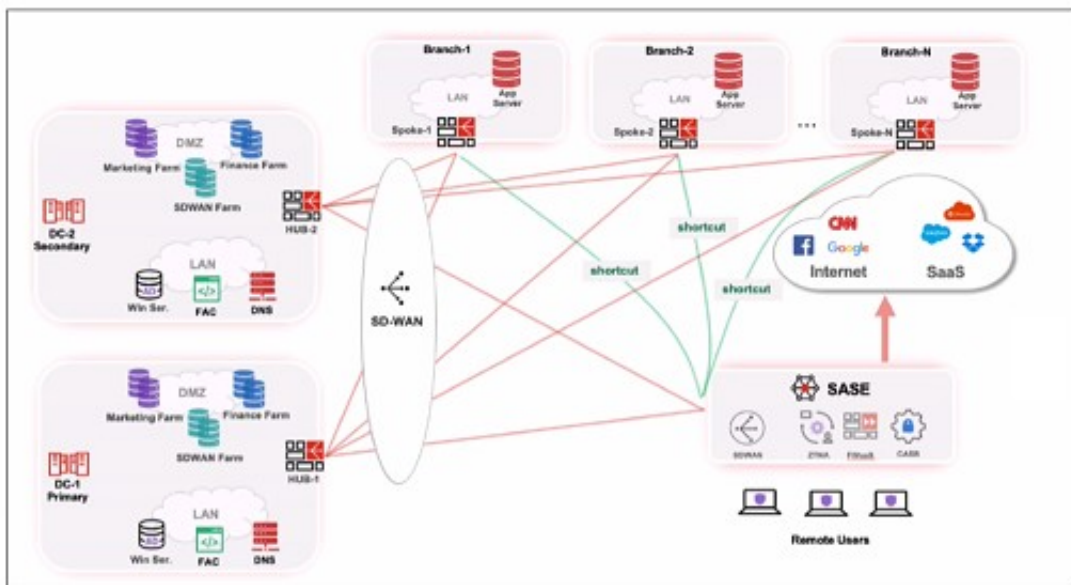
- A. 3
- B. 4
- C. 2
- D. 1

Answer: B

NEW QUESTION 2

Refer to the exhibits.

Topology



Priority settings

Set Priority ▾		Ashburn - Virginia - USA ▾	
<input type="checkbox"/>	Name	Priority ▲	
<input type="checkbox"/>	HUB-1	P1	<div></div> (Highest Priority)
<input type="checkbox"/>	HUB-2	P2	<div></div>

When remote users connected to FortiSASE require access to internal resources on Branch-2. how will traffic be routed?

- A. FortiSASE will use the SD-WAN capability and determine that traffic will be directed to HUB-2. which will then route traffic to Branch-2.
- B. FortiSASE will use the AD VPN protocol and determine that traffic will be directed to Branch-2 directly, using a static route
- C. FortiSASE will use the SD-WAN capability and determine that traffic will be directed to HUB-1, which will then route traffic to Branch-2.
- D. FortiSASE will use the AD VPN protocol and determine that traffic will be directed to Branch-2 directly, using a dynamic route

Answer: D

NEW QUESTION 3

When accessing the FortiSASE portal for the first time, an administrator must select data center locations for which three FortiSASE components? (Choose three.)

- A. Endpoint management
- B. Points of presence
- C. SD-WAN hub
- D. Logging
- E. Authentication

Answer: ABD

Explanation:

When accessing the FortiSASE portal for the first time, an administrator must select data center locations for the following FortiSASE components:

? Endpoint Management:

? Points of Presence (PoPs):

? Logging:

References:

? FortiOS 7.2 Administration Guide: Details on initial setup and configuration steps for FortiSASE.

? FortiSASE 23.2 Documentation: Explains the importance of selecting data center locations for various FortiSASE components.

NEW QUESTION 4

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:

The agentless remote user internet access use 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 5

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 6

Your organization is currently using FortiSASE for its cybersecurity. They have recently hired a contractor who will work from the HQ office and who needs temporary internet access in order to set up a web-based point of sale (POS) system.

What is the recommended way to provide internet access to the contractor?

- A. Use FortiClient on the endpoint to manage internet access.
- B. Use a proxy auto-configuration (PAC) file and provide secure web gateway (SWG) service as an explicit web proxy.
- C. Use zero trust network access (ZTNA) and tag the client as an unmanaged endpoint.
- D. Configure a VPN policy on FortiSASE to provide access to the internet.

Answer: C

Explanation:

The recommended way to provide temporary internet access to the contractor is to use Zero Trust Network Access (ZTNA) and tag the client as an unmanaged endpoint. ZTNA ensures that only authorized users and devices can access specific resources, while treating all endpoints as untrusted by default. By tagging the contractor's device as an unmanaged endpoint, you can apply strict access controls and ensure that the contractor has limited access to only the necessary resources (e.g., the web-based POS system) without exposing the internal network to unnecessary risks. Here's why the other options are less suitable:

? A. Use FortiClient on the endpoint to manage internet access: While FortiClient

provides endpoint security and management, it requires installation and configuration on the contractor's device. This may not be feasible for temporary contractors or unmanaged devices.

? B. Use a proxy auto-configuration (PAC) file and provide secure web gateway

(SWG) service as an explicit web proxy: While this approach can control web traffic, it does not provide the granular access control and security posture validation offered by ZTNA. Additionally, managing PAC files can be cumbersome and less secure compared to ZTNA.

? D. Configure a VPN policy on FortiSASE to provide access to the internet: Using a

VPN policy would grant broader access to the network, which is not ideal for a temporary contractor. It increases the risk of unauthorized access to internal resources and does not align with the principle of least privilege.

References:

? Fortinet FCSS FortiSASE Documentation - Zero Trust Network Access (ZTNA) Use Cases

? FortiSASE Administration Guide - Managing Unmanaged Endpoints

=====

NEW QUESTION 7

Which two statements describe a zero trust network access (ZTNA) private access use case? (Choose two.)

- A. The security posture of the device is secure.
- B. All FortiSASE user-based deployments are supported.
- C. All TCP-based applications are supported.
- D. Data center redundancy is offered.

Answer: AC

Explanation:

Zero Trust Network Access (ZTNA) private access use cases focus on providing secure and controlled access to private applications without exposing them to the public internet. The following two statements accurately describe ZTNA private access use cases:

? The security posture of the device is secure (Option A):ZTNA enforces strict access controls based on the principle of least privilege. Before granting access to private applications, ZTNA evaluates the security posture of the device (e.g., whether it is patched, compliant, and free of malware). Only devices that meet the required security standards are granted access, ensuring that the device is secure before allowing private access.

? All TCP-based applications are supported (Option C):ZTNA supports all TCP- based applications, enabling secure access to a wide range of private applications, including legacy systems and custom-built applications. This flexibility makes ZTNA suitable for organizations with diverse application environments.

Here??s why the other options are incorrect:

? B. All FortiSASE user-based deployments are supported:While FortiSASE supports various deployment scenarios, not all user-based deployments are automatically compatible with ZTNA. Specific configurations and requirements must be met to enable ZTNA functionality.

? D. Data center redundancy is offered:Data center redundancy is unrelated to ZTNA private access use cases. Redundancy typically pertains to infrastructure design and failover mechanisms, not access control methodologies like ZTNA.

References:

? Fortinet FCSS FortiSASE Documentation - ZTNA Private Access Overview

? FortiSASE Administration Guide - ZTNA Deployment Best Practices

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

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 11

Refer to the exhibits.

Managed Endpoints

Endpoint	VPN Username	Management Connection	ZTNA Tags (Simple)	FortiClient Version	Vulnerabilities Detected
Win10-Pro	use2@fortinettraininglab	Online	FortiSASE-Compliant	7.0.10.0538	140
Win7-Pro	use1@fortinettraininglab	Online	FortiSASE-Non-Compliant, FortiSASE-Compliant	7.0.8.0427	176

Secure Internet Access Policy

+ Create Edit Delete Search						
	Name	Profile Group	Source	User	Destination	Action
<input type="checkbox"/>	Botnet Deny		all	All VPN Users	Botnet-C&C.Server	Deny
<input type="checkbox"/>	Non-Compliant		FortiSASE-Non-Compliant	All VPN Users	All Internet Traffic	Deny
<input type="checkbox"/>	Web Traffic	SIA	FortiSASE-Compliant	VPN_Users	All Internet Traffic	Accept
<input type="checkbox"/>	Allow-All	Default		All VPN Users	All Internet Traffic	Accept
<input type="checkbox"/>	Implicit Deny		all	All VPN Users	All Internet Traffic	Deny

WiMO-Pro and Win7-Pro are endpoints from the same remote location. WiMO-Pro can access the internet though FortiSASE, while Wm7-Pro can no longer access the internet

Given the exhibits, which reason explains the outage on Wm7-Pro?

- A. The Win7-Pro device posture has changed.
- B. Win7-Pro cannot reach the FortiSASE SSL VPN gateway
- C. The Win7-Pro FortiClient version does not match the FortiSASE endpoint requirement.
- D. Win-7 Pro has exceeded the total vulnerability detected threshold.

Answer: D

Explanation:

Based on the provided exhibits, the reason why the Win7-Pro endpoint can no longer access the internet through FortiSASE is due to exceeding the total vulnerability detected threshold. This threshold is used to determine if a device is compliant with the security requirements to access the network.

? Endpoint Compliance:

? Vulnerability Threshold:

? Impact on Network Access:

References:

? FortiOS 7.2 Administration Guide: Provides information on endpoint compliance and vulnerability management.

? FortiSASE 23.2 Documentation: Explains how vulnerability thresholds are used to determine endpoint compliance and access control.

NEW QUESTION 12

An organization wants to block all video and audio application traffic but grant access to videos from CNN Which application override action must you configure in the Application Control with Inline-CASB?

- A. Allow
- B. Pass
- C. Permit
- D. Exempt

Answer: A

Explanation:

(<https://docs.fortinet.com/document/fortisase/24.4.75/sia-agent-based-deployment-guide/568255/configuring-application-control-profile>)

NEW QUESTION 16

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 17

.....

Relate Links

100% Pass Your FCSS_SASE_AD-24 Exam with ExamBible Prep Materials

https://www.exambible.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.exambible.com/>