Fortinet

Exam Questions FCSS_SASE_AD-24

FCSS - FortiSASE 24 Administrator

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
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 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 policy type is used to control traffic between the FortiClient endpoint to FortiSASE for secure internet access?

A. VPN policy
B. thin edge policy
C. private access policy
D. secure web gateway (SWG) policy

Answer: A

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
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 useZero 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 thegranular 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 secure internet access (SIA) use case minimizes individual workstation or device setup, because you do not need to install FortiClient on endpoints or configure explicit web proxy settings on web browser-based end points?

A. SIA for inline-CASB users
B. SIA for agentless remote users
C. SIA for SSLVPN remote users
D. SIA for site-based remote users

Answer: B

Explanation:
The Secure Internet Access (SIA) use case that minimizes individual workstation or device setup is SIA for agentless remote users. This use case does not require installing FortiClient on endpoints or configuring explicit web proxy settings on web browser-based endpoints, making it the simplest and most efficient deployment.
? SIA for Agentless Remote Users:
? Minimized Setup:

References:
? FortiOS 7.2 Administration Guide: Details on different SIA deployment use cases and configurations.
? FortiSASE 23.2 Documentation: Explains how SIA for agentless remote users is implemented and the benefits it provides.

NEW QUESTION 10

......

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/