

Exam Questions FCSS_SASE_AD-23

FCSS FortiSASE 23 Administrator

https://www.2passeasy.com/dumps/FCSS_SASE_AD-23/



NEW QUESTION 1

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 2

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 3

Refer to the exhibits.

Managed Endpoints

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

Secure Internet Access Policy

	Name	Profile Group	Source	User	Destination	Action
<input checked="" 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 through 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 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: D

Explanation:

The Secure Web Gateway (SWG) policy is used to control traffic between the FortiClient endpoint and FortiSASE for secure internet access. SWG provides comprehensive web security by enforcing policies that manage and monitor user access to the internet.

? Secure Web Gateway (SWG) Policy:

? Traffic Control:

References:

? FortiOS 7.2 Administration Guide: Details on configuring and managing SWG policies.

? FortiSASE 23.2 Documentation: Explains the role of SWG in securing internet access for endpoints.

NEW QUESTION 5

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 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

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 8

An organization needs to resolve internal hostnames using its internal rather than public DNS servers for remotely connected endpoints. Which two components must be configured on FortiSASE to achieve this? (Choose two.)

- A. SSL deep inspection
- B. Split DNS rules
- C. Split tunnelling destinations
- D. DNS filter

Answer: BC

Explanation:

To resolve internal hostnames using internal DNS servers for remotely connected endpoints, the following two components must be configured on FortiSASE:

? Split DNS Rules:

? Split Tunneling Destinations:

References:

? FortiOS 7.2 Administration Guide: Provides details on configuring split DNS and split tunneling for VPN clients.

? FortiSASE 23.2 Documentation: Explains the implementation and configuration of split DNS and split tunneling for securely resolving internal hostnames.

NEW QUESTION 9

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.

NEW QUESTION 10

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: ABC

Explanation:

To configure a Secure Private Access (SPA) solution to share endpoint information between FortiSASE and a corporate FortiGate, you need to take the following steps:

? Add the FortiGate IP address in the secure private access configuration on

FortiSASE:

? Use the FortiClient EMS cloud connector on the corporate FortiGate to connect to FortiSASE:

? Register FortiGate and FortiSASE under the same FortiCloud account:

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 10

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 15

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_SASE_AD-23 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_SASE_AD-23 Product From:

https://www.2passeasy.com/dumps/FCSS_SASE_AD-23/

Money Back Guarantee

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