Vendor: Fortinet

Exam Code: FCSS_SASE_AD-23

Exam Name: FCSS - FortiSASE 23 Administrator

Version: DEMO

QUESTION 1
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:
FortiSASE can evaluate the security posture of endpoints by checking for compliance with security policies, such as antivirus status, patch levels, and configuration settings. This ensures that only compliant and secure devices are granted access to the network.
Zero Trust Network Access (ZTNA):
ZTNA is based on the principle of "never trust, always verify," which requires continuous assessment of user and device trustworthiness.
FortiSASE plays a crucial role in implementing ZTNA by performing these security posture checks and enforcing access control policies.

QUESTION 2
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:
Agent-based clients can perform vulnerability scans on endpoints to identify and remediate security weaknesses.
This proactive approach helps to ensure that endpoints are secure and compliant with security policies.
SSL Inspection:
Agent-based clients can perform SSL inspection to decrypt and inspect encrypted traffic for threats. This feature is critical for detecting malicious activities hidden within SSL/TLS encrypted traffic.
Web Filter:
Web filtering is a key feature available with agent-based clients, allowing administrators to control and monitor web access.
This feature helps enforce acceptable use policies and protect users from web-based threats.

QUESTION 3
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):
ZTNA ensures that only authenticated and authorized users and devices can access applications.
It applies the principle of least privilege by granting access only to the resources required by the user, minimizing the potential for unauthorized access.
Implementation:
ZTNA continuously verifies user and device trustworthiness and enforces granular access control policies.
This approach enhances security by reducing the attack surface and limiting lateral movement within the network.

QUESTION 4
Which two components are part of onboarding a secure web gateway (SWG) endpoint? (Choose two)

A. FortiSASE CA certificate
B. proxy auto-configuration (PAC) file
C. FortiSASE invitation code
D. FortiClient installer

Answer: AB
Explanation:
Onboarding a Secure Web Gateway (SWG) endpoint involves several components to ensure secure and effective integration with FortiSASE. Two key components are the FortiSASE CA certificate and the proxy auto-configuration (PAC) file.
FortiSASE CA Certificate:
The FortiSASE CA certificate is essential for establishing trust between the endpoint and the FortiSASE infrastructure.
It ensures that the endpoint can securely communicate with FortiSASE services and inspect SSL/TLS traffic.
Proxy Auto-Configuration (PAC) File:
The PAC file is used to configure the endpoint to direct web traffic through the FortiSASE proxy. It provides instructions on how to route traffic, ensuring that all web requests are properly inspected and filtered by FortiSASE.

QUESTION 5
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):
ZTNA operates on the principle of "never trust, always verify," continuously verifying user identity and device security posture before granting access.
It provides secure and granular access to specific applications, ensuring that remote users can securely access the TCP-based application hosted on the private web server.
Secure and Efficient Access:
ZTNA private access allows remote users to connect directly to the application without needing a full VPN tunnel, reducing latency and improving performance. It ensures that only authorized users can access the application, providing robust security controls.

QUESTION 6
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:
Agentless deployment allows remote users to connect to the SIA service without needing to install any client software or configure browser settings.
This approach reduces the setup and maintenance overhead for both users and administrators.
Minimized Setup:
Without the need for FortiClient installation or explicit proxy configuration, the deployment is straightforward and quick.
Users can securely access the internet with minimal disruption and administrative effort.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**