Free Questions for FCSS_SASE_AD-23 by actualtestdumps

Shared by Workman on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

Daily report for application usage

FORTINET

User Productivity

Application Usage

The FortiGuard research team categorizes applications into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application control. FortiGuard maintains thousands of application sensors and can even perform deep application inspection. For example, IT managers can get unprecedented visibility into filenames sent to the cloud or the titles of videos being streamed.

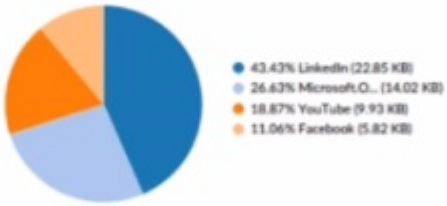
For application category details, see: http://www.fortiguard.com/encyclopedia/application

App Categories

Unknown	41.81%
Web.Client	22.86%
Network.Service	15.14%
General.Interest	12.00%
Collaboration	6.23%
Update	1.50%
Video/Audio	0.21%
Social.Media	0.18%
Email	0.07%

With the proliferation of cloud-based computing, enterprises are increasingly reliant on third parties for infrastructure plumbing. Unfortunately for enterprises, this means that their information is only as secure as the cloud provider's security. In addition, it can often introduce redundancy (if services are already available internally) and increase costs (if not monitored properly).

Cloud Usage (SaaS)



IT managers are often unaware of how many cloud-based services are in use within their organization. Sometimes, these applications can be used to circumvent or even replace corporate infrastructure already available to users in lieu of ease of use. Unfortunately, a potential side effect of this is that your sensitive corporate information could be transferred to the cloud. Accordingly, your data could be exposed if the cloud provider's security infrastructure is breached.

The adoption of "infrastructure as a service" (IaaS) platforms is popular and can be very useful when compute resources are limited or have specialized requirements. That said, the effective outsourcing of your infrastructure must be well regulated to prevent misuse. The occasional auditing of IaaS applications can be a useful exercise not only for security purposes, but also to minimize organizational costs associated with pay per use models or recurring subscription fees.

Cloud Usage (IaaS)

No matching log data for this report

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.)

Options:

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:

A, D

Explanation:

The unusually high number of unknown applications by category in the daily report for application usage can be attributed to the following reasons:

Certificate Inspection is not being used to scan application traffic:

Without certificate inspection, encrypted traffic cannot be adequately analyzed, leading to a higher number of unknown applications.

Certificate inspection allows the FortiSASE to decrypt and inspect HTTPS traffic, identifying applications correctly.

Deep Inspection is not being used to scan traffic:

Deep inspection goes beyond basic traffic analysis, performing thorough examination of packet contents to identify applications accurately.

If deep inspection is not enabled, many applications may go unrecognized and categorized as unknown.

FortiOS 7.2 Administration Guide: Details on certificate inspection and deep inspection configurations.

FortiSASE 23.2 Documentation: Explains the importance of deep inspection and certificate inspection in accurate application identification.

Question 2

Question Type: **MultipleChoice**

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.)

Options:

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:

A, B, C

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:

This step allows FortiSASE to recognize and establish a connection with the corporate FortiGate.

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

The EMS (Endpoint Management Server) cloud connector facilitates the integration between FortiClient endpoints and FortiSASE, enabling seamless sharing of endpoint information.

Register FortiGate and FortiSASE under the same FortiCloud account:

By registering both FortiGate and FortiSASE under the same FortiCloud account, you ensure centralized management and synchronization of configurations and policies.

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.

Question 3

Question Type: **MultipleChoice**

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?

Options:

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):

BGP is widely used for establishing routing adjacencies between different networks, particularly in SD-WAN environments.

It provides scalability and flexibility in managing dynamic routing between FortiSASE and the FortiGate SD-WAN hub.

Routing Adjacency:

BGP enables the exchange of routing information between FortiSASE and the FortiGate SD-WAN hub.

This ensures optimal routing paths and efficient traffic management across the hybrid network.

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.

Question 4

Question Type: **MultipleChoice**

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

Options:

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):

SWG provides comprehensive web security by inspecting and filtering web traffic to protect against web-based threats.

It ensures that all web traffic, whether originating from on-premises or remote locations, is inspected and secured by the cloud-based proxy.

Inline Cloud Access Security Broker (CASB):

CASB enhances security by providing visibility and control over cloud applications and services.

Inline CASB integrates with SWG to enforce security policies for cloud application usage, preventing unauthorized access and data leakage.

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.

Question 5

Question Type: MultipleChoice

Refer to the exhibits.

Managed Endpoints

Endpoint	VPN Username	Management Connection	ZTNA Tags (Simple)	FortiClient Version	Vulnerabilities Detected
Win10-Pro	user2@fortinettraining.lab	Online	FortiSASE-Compliant	7.0.10.0538	140
Win7-Pro	user1@fortinettraining.lab	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
Botnet Deny		all	All VPN Users	Botnet-C&C.Server	Deny
Non-Compliant		FortiSASE-Non-Compliant	All VPN Users	All Internet Traffic	Deny
Web Traffic	SIA	FortiSASE-Compliant	VPN_Users	All Internet Traffic	Accept
Allow-All	Default		All VPN Users	All Internet Traffic	Accept
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?

Options:

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:

FortiSASE monitors endpoint compliance by assessing various security parameters, including the number of vulnerabilities detected on the device.

The compliance status is indicated by the ZTNA tags and the vulnerabilities detected.

Vulnerability Threshold:

The exhibit shows that Win7-Pro has 176 vulnerabilities detected, whereas Win10-Pro has 140 vulnerabilities.

If the endpoint exceeds a predefined vulnerability threshold, it may be restricted from accessing the network to ensure overall network security.

Impact on Network Access:

Since Win7-Pro has exceeded the vulnerability threshold, it is marked as non-compliant and subsequently loses internet access through FortiSASE.

The FortiSASE endpoint profile enforces this compliance check to prevent potentially vulnerable devices from accessing the internet.

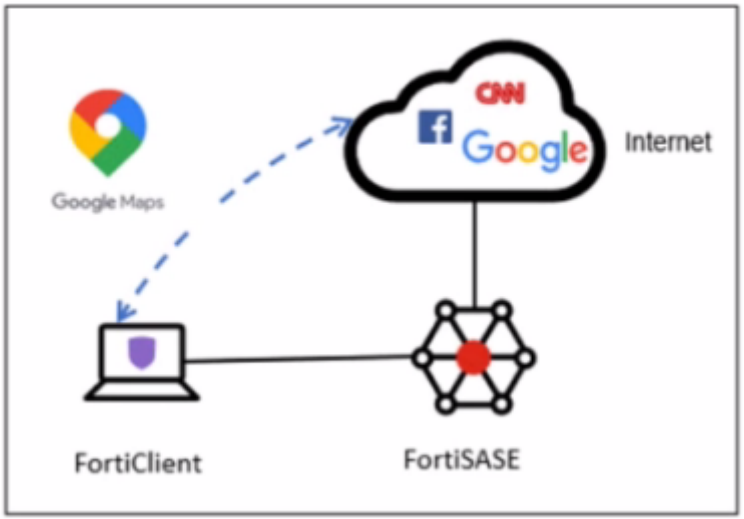
FortiOS 7.2 Administration Guide: Provides information on endpoint compliance and vulnerability management.

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

Question 6

Question Type: **MultipleChoice**

Refer to the exhibit.



A company has a requirement to inspect all the endpoint internet traffic on FortiSASE, and exclude Google Maps traffic from the FortiSASE VPN tunnel and redirect it to the endpoint physical Interface.

Which configuration must you apply to achieve this requirement?

Options:

A- Exempt the Google Maps FQDN from the endpoint system proxy settings.

B- Configure a static route with the Google Maps FQDN on the endpoint to redirect traffic

C- Configure the Google Maps FQDN as a split tunneling destination on the FortiSASE endpoint profile.

D- Change the default DNS server configuration on FortiSASE to use the endpoint system DNS.

Answer:

C

Explanation:

To meet the requirement of inspecting all endpoint internet traffic on FortiSASE while excluding Google Maps traffic from the FortiSASE VPN tunnel and redirecting it to the endpoint's physical interface, you should configure split tunneling. Split tunneling allows specific traffic to bypass the VPN tunnel and be routed directly through the endpoint's local interface.

Split Tunneling Configuration:

Split tunneling enables selective traffic to be routed outside the VPN tunnel.

By configuring the Google Maps Fully Qualified Domain Name (FQDN) as a split tunneling destination, you ensure that traffic to Google Maps bypasses the VPN tunnel and uses the endpoint's local interface instead.

Implementation Steps:

Access the FortiSASE endpoint profile configuration.

Add the Google Maps FQDN to the split tunneling destinations list.

This configuration directs traffic intended for Google Maps to bypass the VPN tunnel and be routed directly through the endpoint's physical network interface.

FortiOS 7.2 Administration Guide: Provides details on split tunneling configuration.

FortiSASE 23.2 Documentation: Explains how to set up and manage split tunneling for specific destinations.

Question 7

Question Type: **MultipleChoice**

How does FortiSASE hide user information when viewing and analyzing logs?

Options:

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:

Hashing data involves converting it into a fixed-size string of characters, which is typically a hash value.

Salting adds random data to the input of the hash function, ensuring that even identical inputs produce different hash values.

This method provides enhanced security by making it more difficult to reverse-engineer the original data from the hash value.

Security and Privacy:

Using salted hashes ensures that user information remains secure and private when stored or analyzed in logs.

This technique is widely used in security systems to protect sensitive data from unauthorized access.

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.

Question 8

Question Type: MultipleChoice

Which two deployment methods are used to connect a FortiExtender as a FortiSASE LAN extension? (Choose two.)

Options:

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:

A, C

Explanation:

There are two deployment methods used to connect a FortiExtender as a FortiSASE LAN extension:

Connect FortiExtender to FortiSASE using FortiZTP:

FortiZero Touch Provisioning (FortiZTP) simplifies the deployment process by allowing FortiExtender to automatically connect and configure itself with FortiSASE.

This method requires minimal manual configuration, making it efficient for large-scale deployments.

Enter the FortiSASE domain name in the FortiExtender GUI as a static discovery server:

Manually configuring the FortiSASE domain name in the FortiExtender GUI allows the extender to discover and connect to the FortiSASE infrastructure.

This static discovery method ensures that FortiExtender can establish a connection with FortiSASE using the provided domain name.

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.

Question 9

Question Type: MultipleChoice

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

Options:

A- FortiSASE CA certificate

B- proxy auto-configuration (PAC) file

C- FortiSASE invitation code

D- FortiClient installer

Answer:

A, B

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.

FortiOS 7.2 Administration Guide: Details on onboarding endpoints and configuring SWG.

FortiSASE 23.2 Documentation: Explains the components required for integrating endpoints with FortiSASE and the process for deploying the CA certificate and PAC file.

Question 10

Question Type: **MultipleChoice**

Which FortiSASE feature ensures least-privileged user access to all applications?

Options:

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.

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.

Question 11

Question Type: MultipleChoice

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

Options:

A- Vulnerability scan

B- SSL inspection

C- Anti-ransomware protection

D- Web filter

E- ZTNA tags

Answer:

A, B, D

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.

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.