

Free Questions for FCSS_SASE_AD-23

Shared by Hansen on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which role does FortiSASE play in supporting zero trust network access (ZTNA) principles?

Options:

- 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.

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.

Question 2

Question Type: MultipleChoice

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

Options:

- 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:

SWG policies are designed to protect users from web-based threats and enforce acceptable use policies.

These policies control and monitor user traffic to and from the internet, ensuring that security protocols are followed.

Traffic Control:

The SWG policy intercepts all web traffic, inspects it, and applies security rules before allowing or blocking access.

This policy type is crucial for providing secure internet access to users connecting through FortiSASE.

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.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.

Security Logs

Log Details ✕

Destination

Destination IP	151.101.40.81
Destination Port	443
Destination Country/Region	United States
Traffic Type	🌐 Internet Access
Destination UUID	4a501662-f85f-51ed-5194-7e45b3d369cd
Hostname	www.bbc.com
URL	https://www.bbc.com/

Application Control

Action

Action	🚫 Blocked
Threat	16,777,216
Policy ID	8
Policy UUID	7d56f000-b41e-51ee-f96b-d0b4d9fb3c2b
Policy Type	policy

Security

Web Filter

Profile Group	🌐 SIA (Internet Access)
Request Type	direct
Direction	incoming
Banned Word	fight
Message	URL was blocked because it contained banned word(s).

To allow access, which web filter configuration must you change on FortiSASE?

Options:

- A- FortiGuard category-based filter
- B- content filter
- C- URL Filter
- D- inline cloud access security broker (CASB) headers

Answer:

C

Explanation:

The exhibit indicates that the URL <https://www.bbc.com/> is being blocked due to containing a banned word ('fight'). To allow access to this specific URL, you need to adjust the URL filter settings on FortiSASE.

URL Filtering:

URL filtering allows administrators to define policies that block or allow access to specific URLs or URL patterns.

In this case, the URL filter is set to block any URL containing the word 'fight.'

Modifying URL Filter:

Navigate to the Web Filter configuration in FortiSASE.

Locate the URL filter settings.

Add an exception for the URL <https://www.bbc.com/> to allow access, even if it contains a banned word.

Alternatively, remove or adjust the banned word list to exclude the word 'fight' if it's not critical to the security policy.

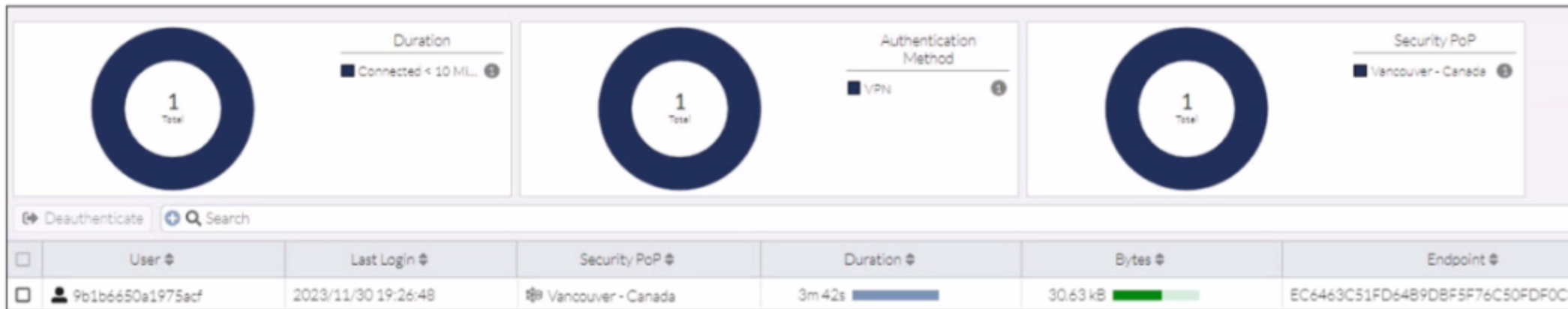
FortiOS 7.2 Administration Guide: Provides details on configuring and managing URL filters.

FortiSASE 23.2 Documentation: Explains how to set up and modify web filtering policies, including URL filters.

Question 4

Question Type: MultipleChoice

Refer to the exhibit.



In the user connection monitor, the FortiSASE administrator notices the user name is showing random characters. Which configuration change must the administrator make to get proper user information?

Options:

- A- Turn off log anonymization on FortiSASE.
- B- Add more endpoint licenses on FortiSASE.
- C- Configure the username using FortiSASE naming convention.
- D- Change the deployment type from SWG to VPN.

Answer:

A

Explanation:

In the user connection monitor, the random characters shown for the username indicate that log anonymization is enabled. Log anonymization is a feature that hides the actual user information in the logs for privacy and security reasons. To display proper user information, you need to disable log anonymization.

Log Anonymization:

When log anonymization is turned on, the actual usernames are replaced with random characters to protect user privacy.

This feature can be beneficial in certain environments but can cause issues when detailed user monitoring is required.

Disabling Log Anonymization:

Navigate to the FortiSASE settings.

Locate the log settings section.

Disable the log anonymization feature to ensure that actual usernames are displayed in the logs and user connection monitors.

FortiSASE 23.2 Documentation: Provides detailed steps on enabling and disabling log anonymization.

Fortinet Knowledge Base: Explains the impact of log anonymization on user monitoring and logging.

Question 5

Question Type: MultipleChoice

What are two advantages of using zero-trust tags? (Choose two.)

Options:

- A-** Zero-trust tags can be used to allow or deny access to network resources
- B-** Zero-trust tags can determine the security posture of an endpoint.
- C-** Zero-trust tags can be used to create multiple endpoint profiles which can be applied to different endpoints
- D-** Zero-trust tags can be used to allow secure web gateway (SWG) access

Answer:

A, B

Explanation:

Zero-trust tags are critical in implementing zero-trust network access (ZTNA) policies. Here are the two key advantages of using zero-trust tags:

Access Control (Allow or Deny):

Zero-trust tags can be used to define policies that either allow or deny access to specific network resources based on the tag associated with the user or device.

This granular control ensures that only authorized users or devices with the appropriate tags can access sensitive resources, thereby enhancing security.

Determining Security Posture:

Zero-trust tags can be utilized to assess and determine the security posture of an endpoint.

Based on the assigned tags, FortiSASE can evaluate the device's compliance with security policies, such as antivirus status, patch levels, and configuration settings.

Devices that do not meet the required security posture can be restricted from accessing the network or given limited access.

FortiOS 7.2 Administration Guide: Provides detailed information on configuring and using zero-trust tags for access control and security posture assessment.

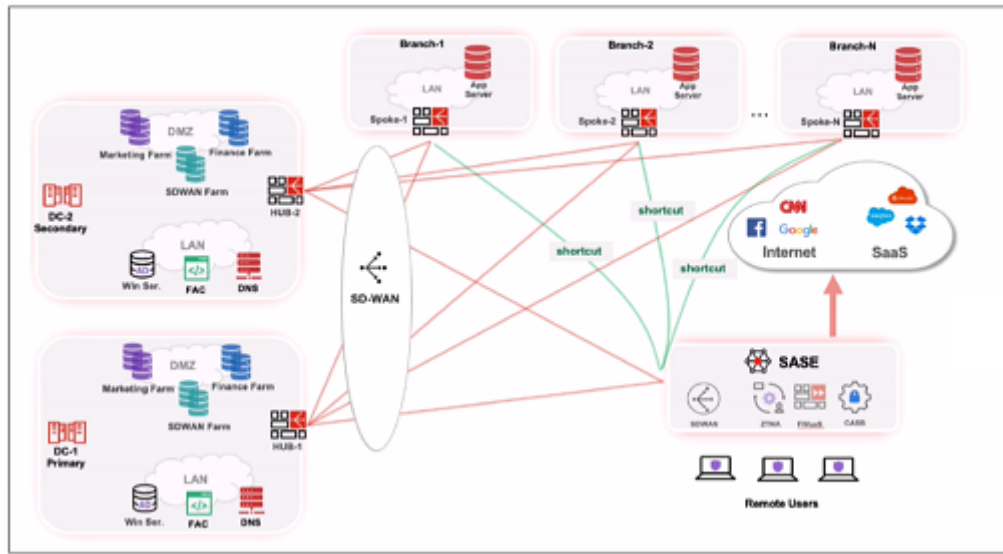
FortiSASE 23.2 Documentation: Explains how zero-trust tags are implemented and used within the FortiSASE environment for enhancing security and compliance.

Question 6

Question Type: MultipleChoice

Refer to the exhibits.

Topology



Priority settings

Set Priority ▾ Ashburn - Virginia - USA ▾

<input type="checkbox"/>	Name	Priority ▲
<input type="checkbox"/>	HUB-1	P1 <input type="range" value="100"/> (Highest Priority)
<input type="checkbox"/>	HUB-2	P2 <input type="range" value="50"/>

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

Options:

- 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:

C

Explanation:

When remote users connected to FortiSASE require access to internal resources on Branch-2, the following process occurs:

SD-WAN Capability:

FortiSASE leverages SD-WAN to optimize traffic routing based on performance metrics and priorities.

In the priority settings, HUB-1 is configured with the highest priority (P1), whereas HUB-2 has a lower priority (P2).

Traffic Routing Decision:

FortiSASE evaluates the available hubs (HUB-1 and HUB-2) and selects HUB-1 due to its highest priority setting.

Once the traffic reaches HUB-1, it is then routed to the appropriate branch based on internal routing policies.

Branch-2 Access:

Since HUB-1 has the highest priority, FortiSASE directs the traffic to HUB-1.

HUB-1 then routes the traffic to Branch-2, providing the remote users access to the internal resources.

FortiOS 7.2 Administration Guide: Details on SD-WAN configurations and priority settings.

FortiSASE 23.2 Documentation: Explains how FortiSASE integrates with SD-WAN to route traffic based on defined priorities and performance metrics.

Question 7

Question Type: MultipleChoice

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?

Options:

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

Answer:

D

Explanation:

To block all video and audio application traffic while granting access to videos from CNN, you need to configure an application override action in the Application Control with Inline-CASB. Here is the step-by-step detailed explanation:

Application Control Configuration:

Application Control is used to identify and manage application traffic based on predefined or custom application signatures.

Inline-CASB (Cloud Access Security Broker) extends these capabilities by allowing more granular control over cloud applications.

Blocking Video and Audio Applications:

To block all video and audio application traffic, you can create a policy within Application Control to deny all categories related to video and audio streaming.

Granting Access to Specific Videos (CNN):

To allow access to videos from CNN specifically, you must create an override rule within the same Application Control profile.

The override action 'Exempt' ensures that traffic to specified URLs (such as those from CNN) is not subjected to the blocking rules set for other video and audio traffic.

Configuration Steps:

Navigate to the Application Control profile in the FortiSASE interface.

Set the application categories related to video and audio streaming to 'Block.'

Add a new override entry for CNN video traffic and set the action to 'Exempt.'

FortiOS 7.2 Administration Guide: Detailed steps on configuring Application Control and Inline-CASB.

Fortinet Training Institute: Provides scenarios and examples of using Application Control with Inline-CASB for specific use cases.

Question 8

Question Type: MultipleChoice

Refer to the exhibits.

Web Filtering logs

	User	Destination P...	Traffic Type	Security Events	Security Action	Log Details
<input checked="" type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	<div style="display: flex; border-bottom: 1px solid #ccc;"> <div style="flex: 1; padding-right: 10px;"> <p>Details</p> </div> <div style="flex: 2; padding-left: 10px;"> <p>Security</p> </div> </div> <p>Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36</p> <p>Category: 50</p> <p>Category Description: Information and Computer Security</p> <p>Direction: outgoing</p> <p>Event Type: ftgd_allow</p> <p>Hostname: www.eicar.org</p> <p>Message: URL belongs to an allowed category in policy</p> <p>Profile Group: SIA (Internet Access)</p> <p>Referrer URI: https://www.eicar.org/download-anti-ai-ware-testfile/</p> <p>Request Type: referral</p> <p>Sub Type: webfilter</p> <p>Type: utm</p> <p>Timezone: -0800</p> <p>URL: https://www.eicar.org/download/eicar-com-zip/?wpdmdl=8847&refresh=650477aha001709126775</p>
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	

Security Profile Group

Rename
 Delete

AntiVirus

Threats	Count	Inspected Protocols
		HTTP ✔
		SMTP ✔
		POP3 ✔
		IMAP ✔
		FTP ✔
		CIFS ✔

View All
 View Logs
 Customize

Web Filter With Inline-CASB

Threats	Count	Filters
www.eicar.org	80	<input checked="" type="checkbox"/> Allow 0
5f3c395.com19.de	22	<input type="checkbox"/> Block 0
www.eicar.com	19	<input type="checkbox"/> Exempt 0
encrypted-tbn0.gstatic.com	9	<input checked="" type="checkbox"/> Monitor 93
ocsp.digicert.com	8	<input type="checkbox"/> Warning 0
		<input type="checkbox"/> Disable 0
		<input checked="" type="checkbox"/> Inline-CASB Headers 1

View All
 View Logs
 Customize

Intrusion Prevention

Threats	Count	Intrusion Prevention
		⚠
<p>Recommended</p> <p><input type="checkbox"/> Scanning traffic for all known threats and applying the recommended settings. Disabled</p>		






View All
 View Logs
 Customize

SSL Inspection

Threats	Count	SSL Inspection
ssl-anomaly	734	<p>Deep Inspection</p> <p><input checked="" type="checkbox"/> SSL connections are decrypted to allow for inspection of the contents.</p> <p><input checked="" type="checkbox"/> Exempt Hosts 1</p> <p><input checked="" type="checkbox"/> Exempt URL Categories 2</p>

View All
 View Logs
 Customize

Secure Internet Access policy

Name 	Web Traffic
Source Scope	All VPN Users Edge Device
Source	All Traffic Specify
User	All VPN Users Specify VPN_Users  +
Destination	All Internet Traffic Specify
Service	ALL  +
Profile Group	Default Specify SIA 
Force Certificate Inspection 	<input checked="" type="checkbox"/>
Action	<input checked="" type="checkbox"/> Accept <input type="checkbox"/> Deny
Status	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable
Logging Options	
Log Allowed Traffic <input checked="" type="checkbox"/>	Security Events All Sessions

A FortiSASE administrator has configured an antivirus profile in the security profile group and applied it to the internet access policy. Remote users are still able to download the eicar.com-zip file from <https://eicar.org>. Traffic logs show traffic is allowed by the policy.

Which configuration on FortiSASE is allowing users to perform the download?

Options:

- A- Web filter is allowing the traffic.
- B- IPS is disabled in the security profile group.
- C- The HTTPS protocol is not enabled in the antivirus profile.
- D- Force certificate inspection is enabled in the policy.

Answer:

A

Explanation:

Based on the provided exhibits and the configuration details, the reason why users are still able to download the eicar.com-zip file despite having an antivirus profile applied is due to the Web Filter allowing the traffic. Here is the step-by-step detailed explanation:

Web Filtering Logs Analysis:

The logs show that the traffic to the destination port 443 (which is HTTPS) is allowed and the security event triggered is Web Filter.

The log details indicate that the URL belongs to an allowed category in the policy and thus, the traffic is permitted by the Web Filter.

Security Profile Group Configuration:

The Web Filter with Inline-CASB section indicates that the site www.eicar.org is being monitored (93 occurrences) and not blocked.

Since the Web Filter is set to allow traffic from this site, the antivirus profile will not block it because the Web Filter decision takes precedence.

Antivirus Profile Configuration:

Although the antivirus profile is configured, the logs do not show any antivirus actions being triggered. This indicates that the web filter is overriding the antivirus action.

Policy Configuration:

The policy named 'Web Traffic' shows that it has logging enabled and is set to accept traffic.

The profile group 'SIA' applied to this policy includes both Web Filter and Antivirus settings. However, since the Web Filter is allowing the traffic, the antivirus profile does not get the chance to inspect it.

FortiGate Security 7.2 Study Guide: Provides details on the precedence of web filtering over antivirus in security profiles.

Fortinet Knowledge Base: Detailed explanation of web filtering and antivirus profiles interaction.

To Get Premium Files for FCSS_SASE_AD-23 Visit

https://www.p2pexams.com/products/fcss_sase_ad-23

For More Free Questions Visit

<https://www.p2pexams.com/fortinet/pdf/fcss-sase-ad-23>

