

Fortinet

Exam Questions FCSS_SASE_AD-23

FCSS FortiSASE 23 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: D

Explanation:

During FortiSASE provisioning, the FortiSASE administrator needs to configure at least one security point of presence (PoP). A single PoP is sufficient to get started with FortiSASE, providing the necessary security services and connectivity for users.

? Security Point of Presence (PoP):

? Scalability:

References:

? FortiOS 7.2 Administration Guide: Provides details on the provisioning process for FortiSASE.

? FortiSASE 23.2 Documentation: Explains the configuration and role of security PoPs in the FortiSASE architecture.

NEW QUESTION 2

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 3

When viewing the daily summary report generated by FortiSASE, the administrator notices that the report contains very little data. What is a possible explanation for this almost empty report?

- A. Digital experience monitoring is not configured.
- B. Log allowed traffic is set to Security Events for all policies.
- C. The web filter security profile is not set to Monitor
- D. There are no security profile group applied to all policies.

Answer: B

Explanation:

If the daily summary report generated by FortiSASE contains very little data, one possible explanation is that the "Log allowed traffic" setting is configured to log only "Security Events" for all policies. This configuration limits the amount of data logged, as it only includes security events and excludes normal allowed traffic.

? Log Allowed Traffic Setting:

? Impact on Report Data:

References:

? FortiOS 7.2 Administration Guide: Provides details on configuring logging settings for traffic policies.

? FortiSASE 23.2 Documentation: Explains the impact of logging configurations on report generation and data visibility.

NEW QUESTION 4

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 5

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?

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

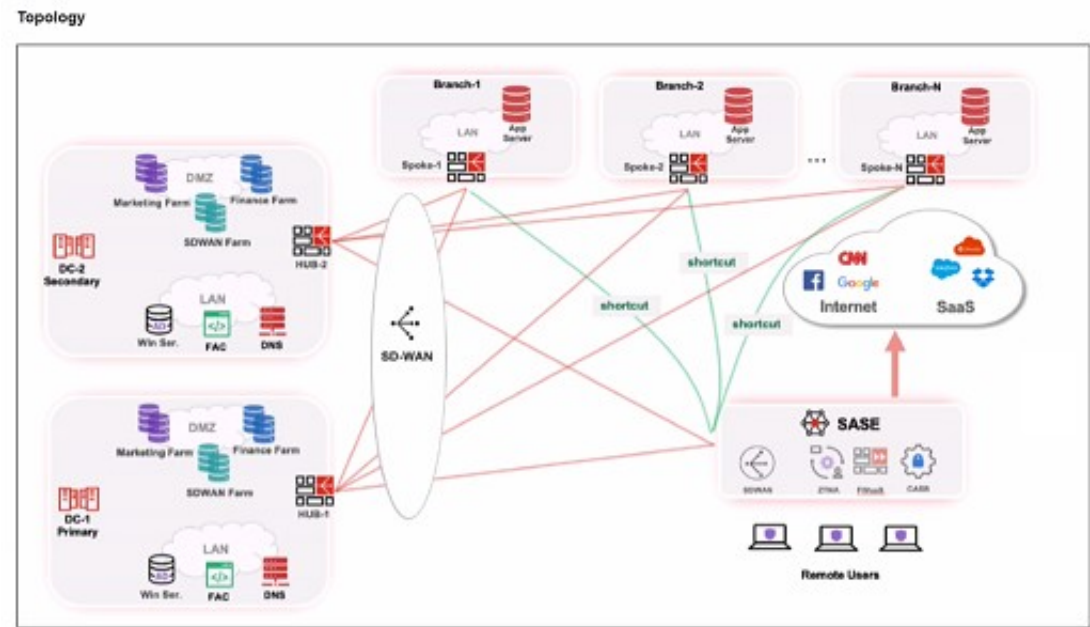
Answer: D

Explanation:

- ? Application Control Configuration:
 - ? Blocking Video and Audio Applications:
 - ? Granting Access to Specific Videos (CNN):
 - ? Configuration Steps:
- References:
- ? 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.

NEW QUESTION 6

Refer to the exhibits.



Priority settings

Set Priority ▾		Ashburn - Virginia - USA ▾	
<input type="checkbox"/>	Name	Priority ▲	
<input type="checkbox"/>	HUB-1	P1	(Highest Priority)
<input type="checkbox"/>	HUB-2	P2	

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

- 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:
 - ? Traffic Routing Decision:
 - ? Branch-2 Access:
- References:
- ? 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.

NEW QUESTION 7

Which two advantages does FortiSASE bring to businesses with multiple branch offices? (Choose two.)

- A. It offers centralized management for simplified administration.
- B. It enables seamless integration with third-party firewalls.
- C. it offers customizable dashboard views for each branch location
- D. It eliminates the need to have an on-premises firewall for each branch.

Answer: AD

Explanation:

FortiSASE brings the following advantages to businesses with multiple branch offices:

? Centralized Management for Simplified Administration:

? Eliminates the Need for On-Premises Firewalls:

References:

? FortiOS 7.2 Administration Guide: Provides information on the benefits of centralized management and cloud-based security solutions.

? FortiSASE 23.2 Documentation: Explains the advantages of using FortiSASE for businesses with multiple branch offices, including reduced need for on-premises firewalls.

NEW QUESTION 8

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	Details Security
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Category 50
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Category Description Information and Computer Security
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Direction outgoing
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Event Type ftgd_allow
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Hostname www.eicar.org
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Message URL belongs to an allowed category in policy
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Profile Group SIA (Internet Access)
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Referrer URI https://www.eicar.org/download-anti-malware-testfile/
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Request Type referral
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Sub Type webfilter
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Type utm
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Timezone -0800
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	URL https://www.eicar.org/download/eicar_com-zip/?vdpdml=8847&refresh=65df3477aha001709126775

Security Profile Group

Rename

Delete

AntiVirus

Threats

Count

Inspected Protocols

View All

View Logs

Customize

Web Filter With Inline-CASB

Threats

Count

Filters

www.eicar.org

80

Allow

0

5f3c395.com19.de

22

Block

0

www.eicar.com

19

Exempt

0

encrypted-tbn0.gstatic.com

9

Monitor

93

ocsp.digicert.com

9

Warning

0

Disable

0

Inline-CASB Headers

1

View All

View Logs

Customize

Intrusion Prevention

Threats

Count

Intrusion Prevention

Recommended

Scanning traffic for all known threats and applying the recommended settings.

Disabled

View All

View Logs

Customize

SSL Inspection

Threats

Count

SSL Inspection

ssl-anomaly

734

Deep Inspection

SSL connections are decrypted to allow for inspection of the contents.

4 Exempt Hosts

1

Exempt URL Categories

2

View All

View Logs

Customize

Secure Internet Access policy

Name ⓘ

Web Traffic

Source Scope

AllVPN UsersEdge Device

Source

All TrafficSpecify

User

All VPN UsersSpecify

👤 VPN_Users

×

+

Destination

All Internet TrafficSpecify

Service

🖥️ ALL

×

+

Profile Group

DefaultSpecify

SIA

Force Certificate Inspection ⓘ

🔵

Action

✓ Accept

🚫 Deny

Status

🟢 Enable

🔴 Disable

Logging Options

Log Allowed Traffic

🔵

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?

- 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:

? Web Filtering Logs Analysis:
? Security Profile Group Configuration:
? Antivirus Profile Configuration:
? Policy Configuration:
References:
? 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.

NEW QUESTION 9

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

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?

- 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:

? Modifying URL Filter:

References:

? 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.

NEW QUESTION 10

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_SASE_AD-23 Practice Test Here](#)