Fortinet

FCSS_SASE_AD-24
Fortinet FCSS - FortiSASE 24 Administrator

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.

https://examsempire.com/

Latest Version: 6.0

Question: 1

Refer to the exhibits.

Web Filtering logs

	User	Destination P...	Traffic Type	Security Events	Security Action
☑	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed
☐	👤 user2@fortinettraining.lab	443	🖧 Internet Access	🔮 Web Filter	✔ Allowed

Log Details ✕

Details | **Security**

Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Category	50
Category Description	Information and Computer Security
Direction	outgoing
Event Type	ftgd_allow
Hostname	www.eicar.org
Message	URL belongs to an allowed category in policy
Profile Group	🖧 SIA (Internet Access)
Referrer URI	https://www.eicar.org/download-anti-malware-testfile/
Request Type	referral
Sub Type	webfilter
Type	utm
Timezone	-0800
URL	https://www.eicar.org/download/eicar_com-zip/?wpdmdl=8847&refresh=65df3477aba001709126775

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	✔ Allow	0
5f3c395.ccm19.de	22	🚫 Block	0
www.eicar.com	19	⊖ Exempt	0
encrypted-tbn0.gstatic.com	9	👁 Monitor	93
ocsp.digicert.com	8	⚠ 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 recommm... 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.	
		🏴 Exempt Hosts	1
		🗂 Exempt URL Categories	2

☰ 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 ⓘ	🔵
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: D

Explanation:

Question: 2

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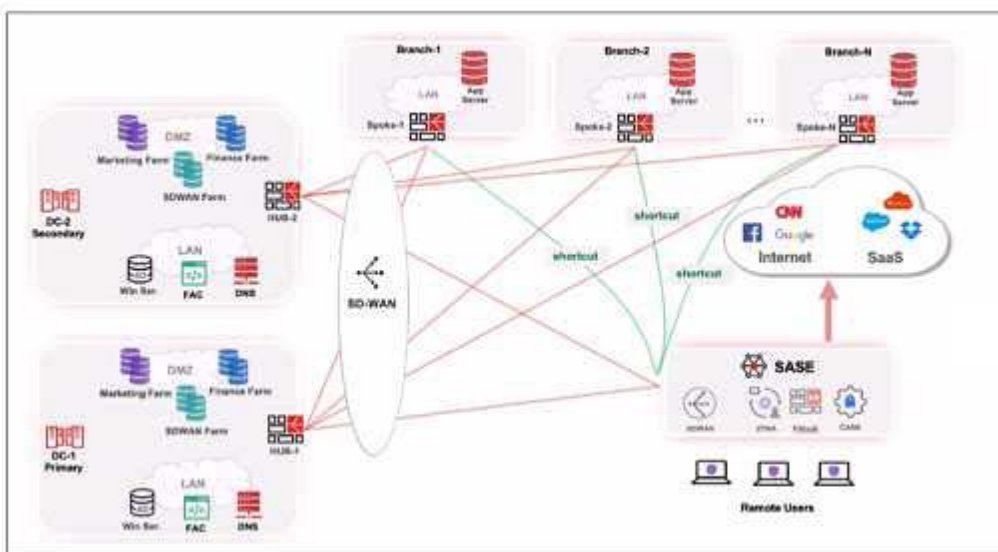
A. Allow
B. Pass
C. Permit
D. Exempt

Answer: A

Explanation:
(https://docs.fortinet.com/document/fortisase/24.4.75/sia-agent-based-deploymentguide/568255/configuring-application-control-profile

Question: 3

Refer to the exhibits.

Priority settings

	Name	Priority ^
☐	HUB-1	P1 ▓▓▓▓▓▓▓▓▓▓▓ (Highest Priority)
☐	HUB-2	P2 ▓▓▓▓▓▓

Set Priority ▾   🕸 Ashburn - Virginia - USA ▾

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: D

Question: 4

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

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: AB

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.

Reference:

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: 5

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?

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.

Reference:

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.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/