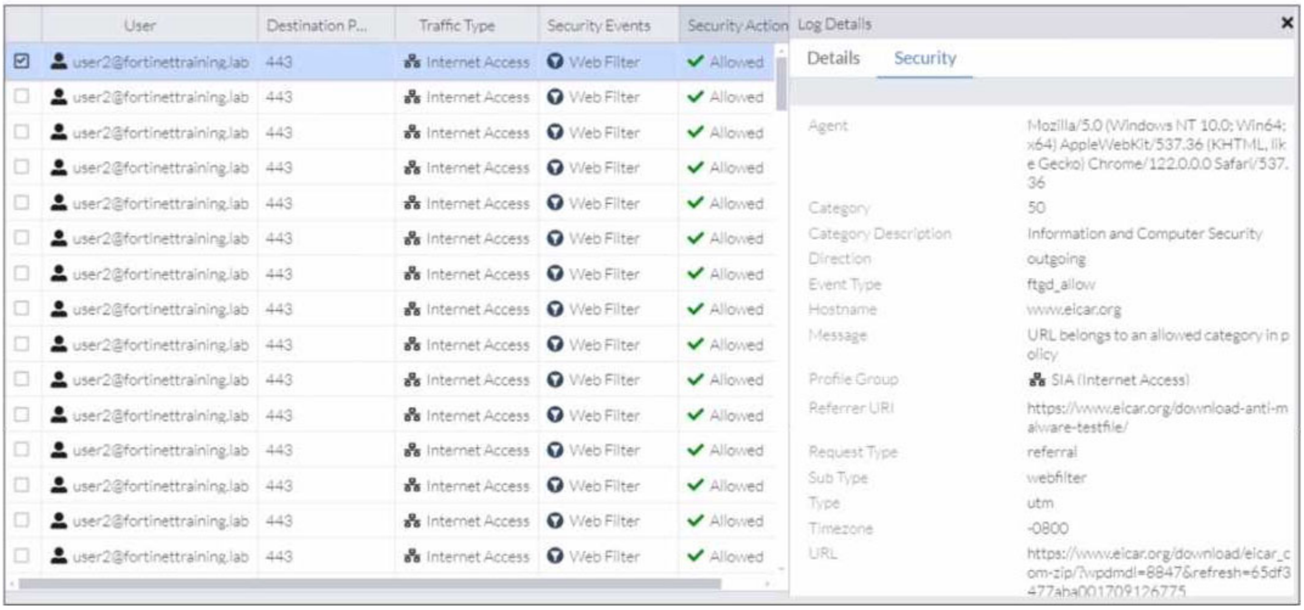
Exam : FCSS_SASE_AD-23

Title : FCSS - FortiSASE 23 Administrator

Version : DEMO

1.Refer to the exhibits.

Web Filtering logs

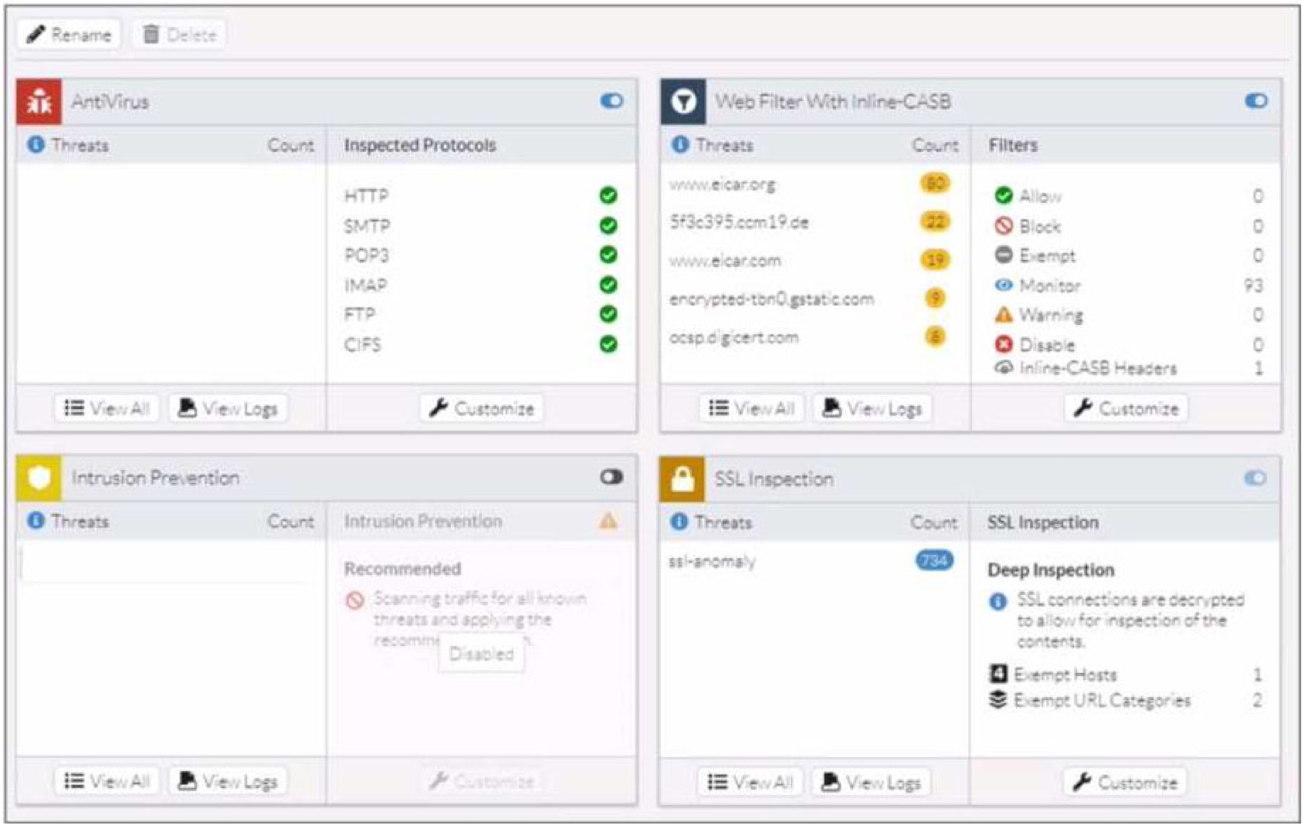


	User	Destination P...	Traffic Type	Security Events	Security Action
☑	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
☐	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
☐	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
☐	user2@fortinettraining.lab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

Log Details

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



AntiVirus

Threats	Count

Inspected Protocols	
HTTP	✓
SMTP	✓
POP3	✓
IMAP	✓
FTP	✓
CIFS	✓

Web Filter With Inline-CASB

Threats	Count
www.eicar.org	80
5f3c395.com19.de	22
www.eicar.com	19
encrypted-tbn0.gstatic.com	9
ocsp.digicert.com	6

Filters	
Allow	0
Block	0
Exempt	0
Monitor	93
Warning	0
Disable	0
Inline-CASB Headers	1

Intrusion Prevention

Threats	Count

Intrusion Prevention

Recommended

Scanning traffic for all known threats and applying the recomm

Disabled

SSL Inspection

Threats	Count
ssl-anomaly	734

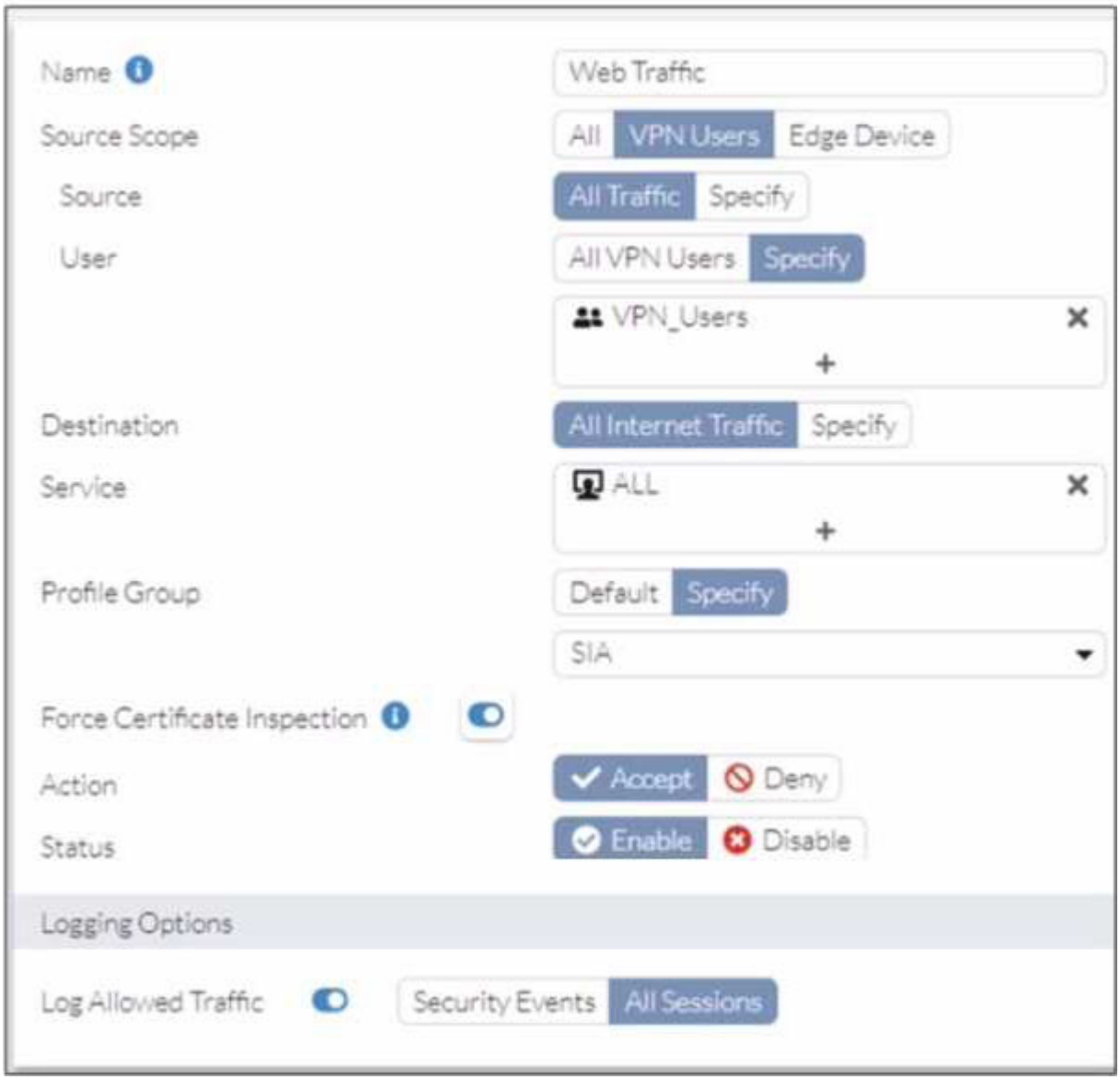
SSL Inspection

Deep Inspection

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

Exempt Hosts	1
Exempt URL Categories	2

Secure Internet Access policy



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:

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:

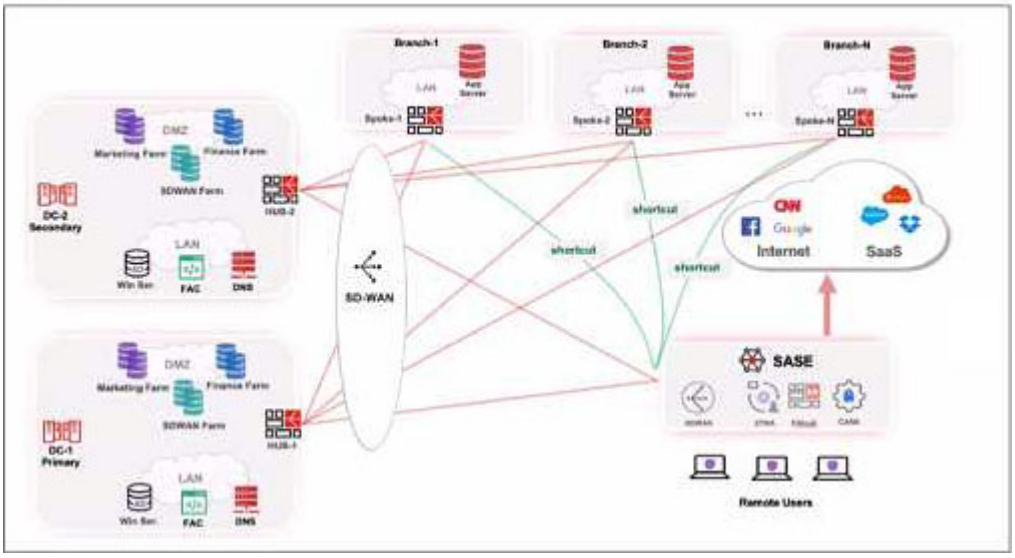
Web Filtering Logs Analysis:
The logs show that the traffic to the destination port 443 (which is HTTPS) is allowed and the security event triggered is Web Filter.
The log details indicate that the URL belongs to an allowed category in the policy and thus, the traffic is permitted by the Web Filter.
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.
Reference: 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.

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: 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

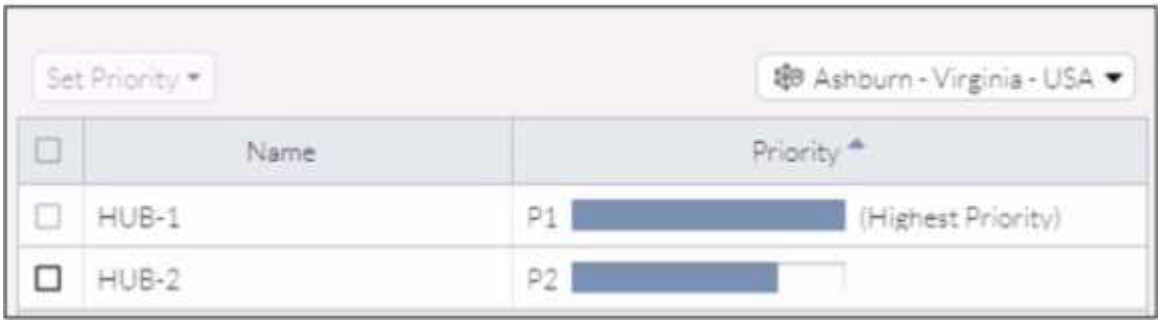
Application Control profile.
The override action "Exempt" ensures that traffic to specified URLs (such as those from CNN) is not subjected to the blocking rules set for other video and audio traffic.
Configuration Steps:
Navigate to the Application Control profile in the FortiSASE interface.
Set the 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."
Reference: 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.

3.Refer to the exhibits.

Topology



Priority settings



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:

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.

Reference: 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.

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.

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.