



TRUSTED, ACCURATE AND RELIABLE!

The most comprehensive IT certification
preparation materials in the industry!

All rights reserved. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. Unauthorized copying, reselling, or distribution of this document is strictly prohibited and may result in legal action.

<https://www.virtulearner.com>
support@virtulearner.com

Fortinet

FCSS_SASE_AD-24

FCSS - FortiSASE 24

Administrator

QUESTION: 1

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	
<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	
<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	

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.elcar.org

Message: URL belongs to an allowed category in policy

Profile Group: SIA (Internet Access)

Referrer URI: https://www.elcar.org/download-anti-malware-testfile/

Request Type: referral

Sub Type: webfilter

Type: utm

Timezone: -0800

URL: https://www.elcar.org/download/elcar_com-zip/?vpdmid=8847&refresh=65df3477aba001709126775

Security Profile Group

The screenshot displays the Palo Alto Networks User Interface with four security modules visible:

- AntiVirus:** Shows a table with columns 'Threats', 'Count', and 'Inspected Protocols'. The protocols listed are HTTP, SMTP, POP3, IMAP, FTP, and CIFS, all with green checkmarks indicating they are inspected.
- Web Filter With Inline-CASB:** Shows a table with columns 'Threats', 'Count', and 'Filters'. The threats listed are www.eican.org (60), 5f3c395.com19.de (22), www.eican.com (19), encrypted-tbn0.gstatic.com (9), and ocp.digicert.com (9). The filters listed are Allow (0), Block (0), Exempt (0), Monitor (93), Warning (0), Disable (0), and Inline-CASB Headers (1).
- Intrusion Prevention:** Shows a table with columns 'Threats', 'Count', and 'Intrusion Prevention'. The 'Recommended' section shows a warning icon and the text 'Scanning traffic for all known threats and applying the recommended rules is Disabled'.
- SSL Inspection:** Shows a table with columns 'Threats', 'Count', and 'SSL Inspection'. The threat listed is ssl-anomaly (734). The 'Deep Inspection' section shows a warning icon and the text 'SSL connections are decrypted to allow for inspection of the contents.'.

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="radio"/> Accept <input type="radio"/> Deny
Status	<input checked="" type="radio"/> Enable <input type="radio"/> 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?

- 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(s): D