Fortinet

Exam Questions FCSS_SASE_AD-23

FCSS FortiSASE 23 Administrator

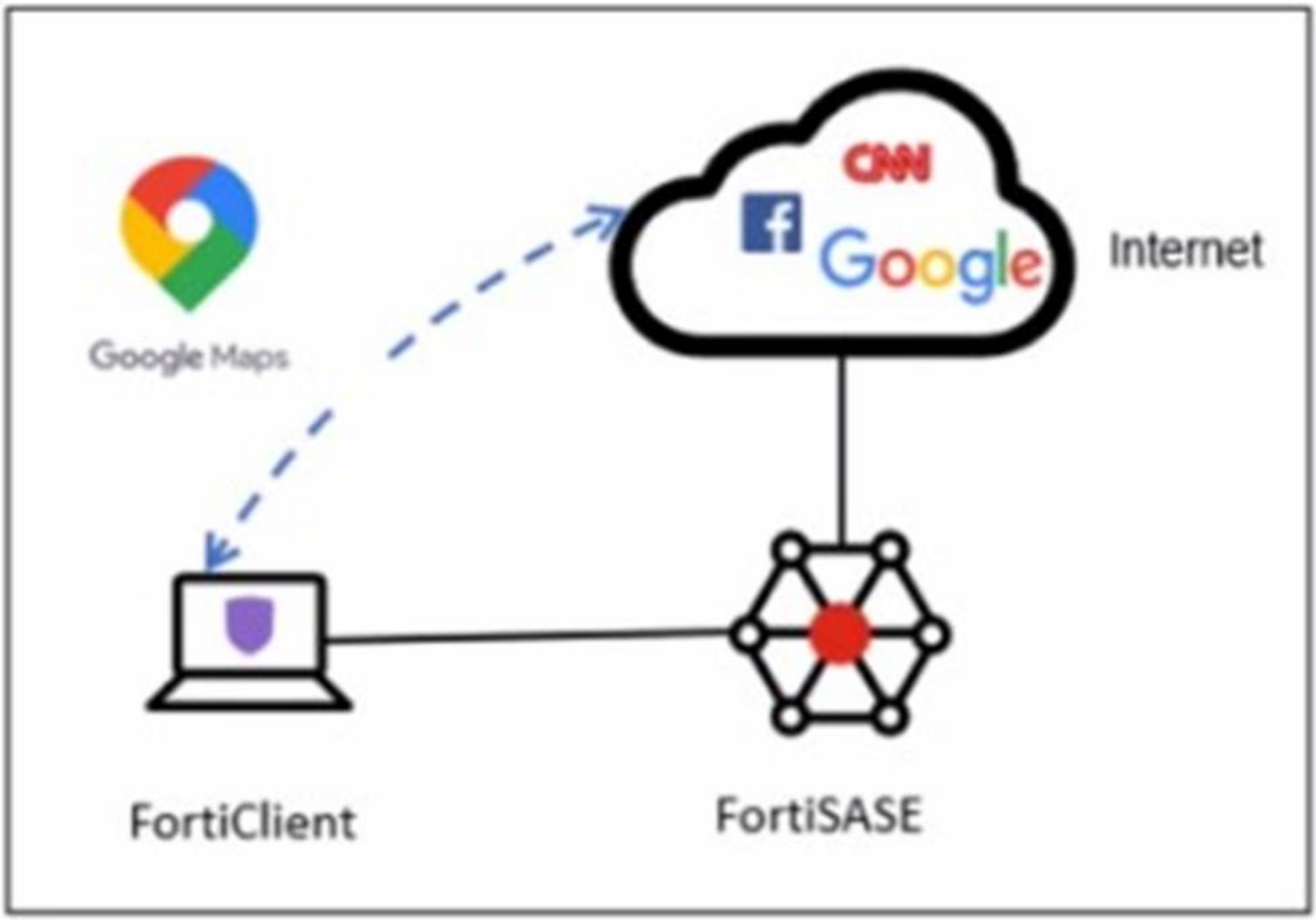
NEW QUESTION 1
To complete their day-to-day operations, remote users require access to a TCP-based application that is hosted on a private web server. Which FortiSASE deployment use case provides the most efficient and secure method for meeting the remote users' requirements?

A. SD-WAN private access
B. inline-CASB
C. zero trust network access (ZTNA) private access
D. next generation firewall (NGFW)

Answer: C

Explanation:
Zero Trust Network Access (ZTNA) private access provides the most efficient and secure method for remote users to access a TCP-based application hosted on a private web server. ZTNA ensures that only authenticated and authorized users can access specific applications based on predefined policies, enhancing security and access control.
? Zero Trust Network Access (ZTNA):
? Secure and Efficient Access:
References:
? FortiOS 7.2 Administration Guide: Provides detailed information on ZTNA and its deployment use cases.
? FortiSASE 23.2 Documentation: Explains how ZTNA can be used to provide secure access to private applications for remote users.

NEW QUESTION 2
Refer to the exhibit.



A company has a requirement to inspect all the endpoint internet traffic on FortiSASE, and exclude Google Maps traffic from the FortiSASE VPN tunnel and redirect it to the endpoint physical Interface.
Which configuration must you apply to achieve this requirement?

A. Exempt the Google Maps FQDN from the endpoint system proxy settings.
B. Configure a static route with the Google Maps FQDN on the endpoint to redirect traffic
C. Configure the Google Maps FQDN as a split tunneling destination on the FortiSASE endpoint profile.
D. Change the default DNS server configuration on FortiSASE to use the endpoint system DNS.

Answer: C

Explanation:
To meet the requirement of inspecting all endpoint internet traffic on FortiSASE while excluding Google Maps traffic from the FortiSASE VPN tunnel and redirecting it to the endpoint's physical interface, you should configure split tunneling. Split tunneling allows specific traffic to bypass the VPN tunnel and be routed directly through the endpoint's local interface.
? Split Tunneling Configuration:

? Implementation Steps:
References:
? FortiOS 7.2 Administration Guide: Provides details on split tunneling configuration.
? FortiSASE 23.2 Documentation: Explains how to set up and manage split tunneling for specific destinations.

NEW QUESTION 3
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:
? Disabling Log Anonymization:
References:
? 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.

NEW QUESTION 4
What are two advantages of using zero-trust tags? (Choose two.)

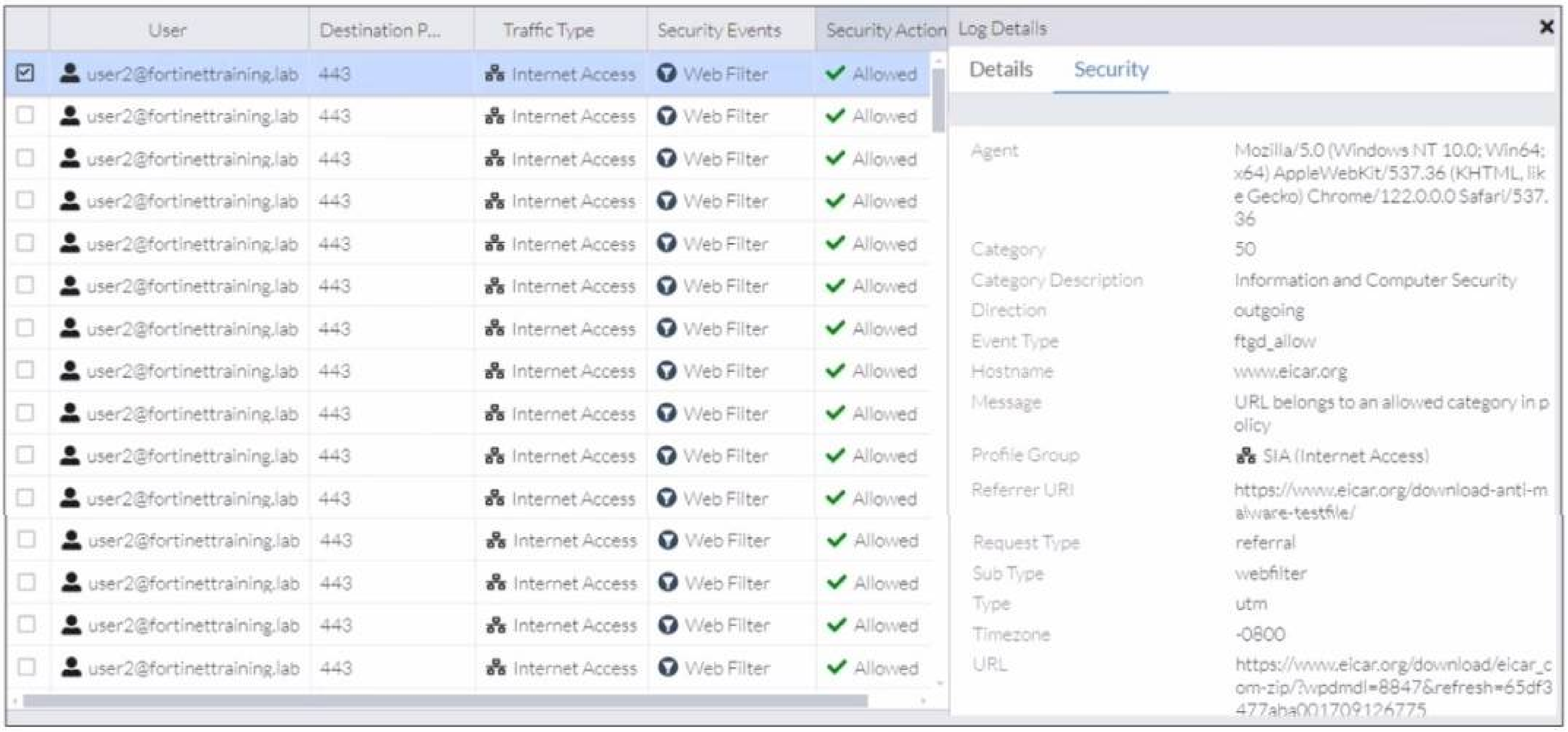
A. Zero-trust tags can be used to allow or deny access to network resources
B. Zero-trust tags can determine the security posture of an endpoint.
C. Zero-trust tags can be used to create multiple endpoint profiles which can be applied to different endpoints
D. Zero-trust tags can be used to allow secure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

Answer: AB

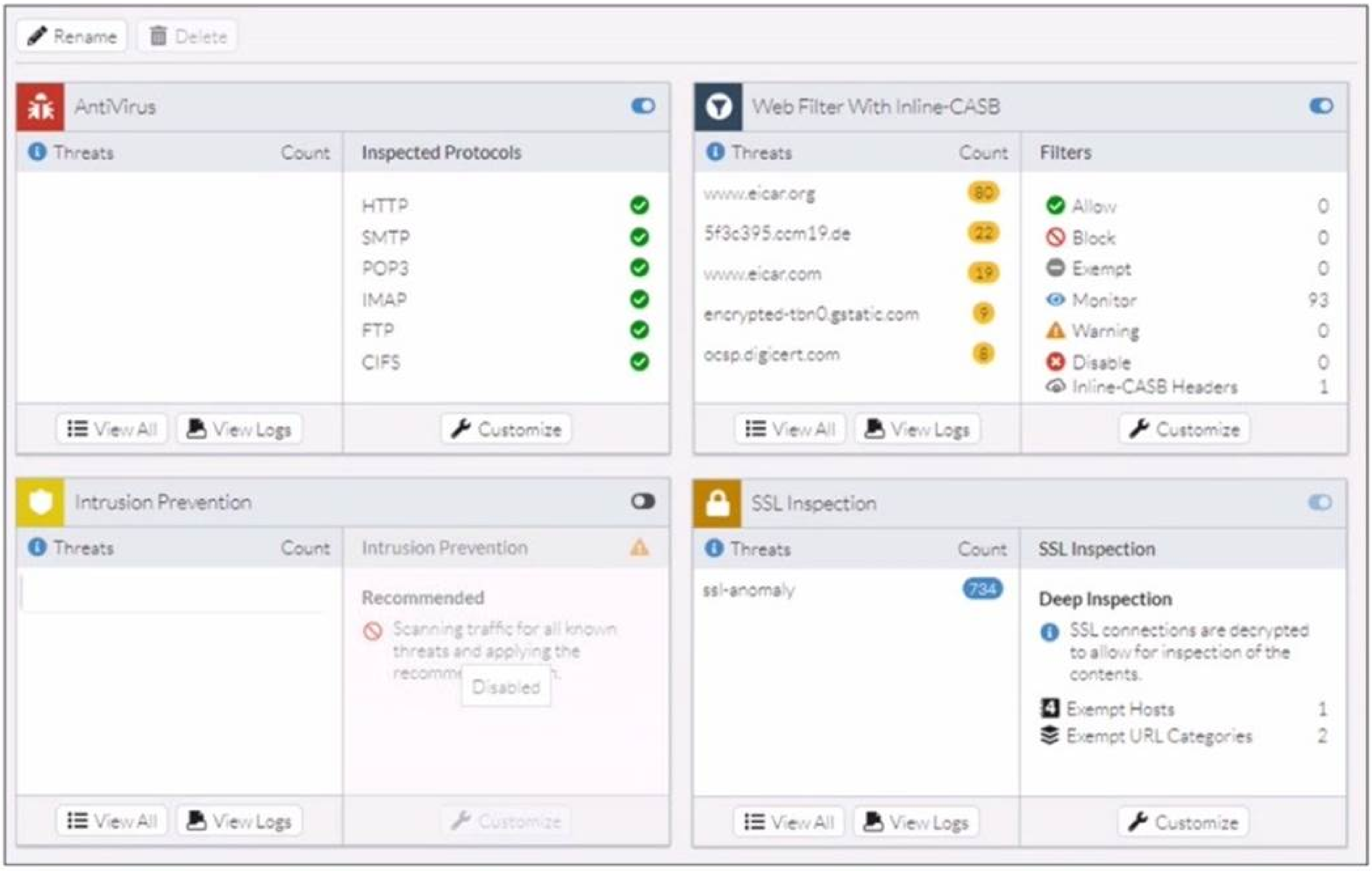
Explanation:
Zero-trust tags are critical in implementing zero-trust network access (ZTNA) policies. Here are the two key advantages of using zero-trust tags:
? Access Control (Allow or Deny):
? Determining Security Posture:
References:
? FortiOS 7.2 Administration Guide: Provides detailed information 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.

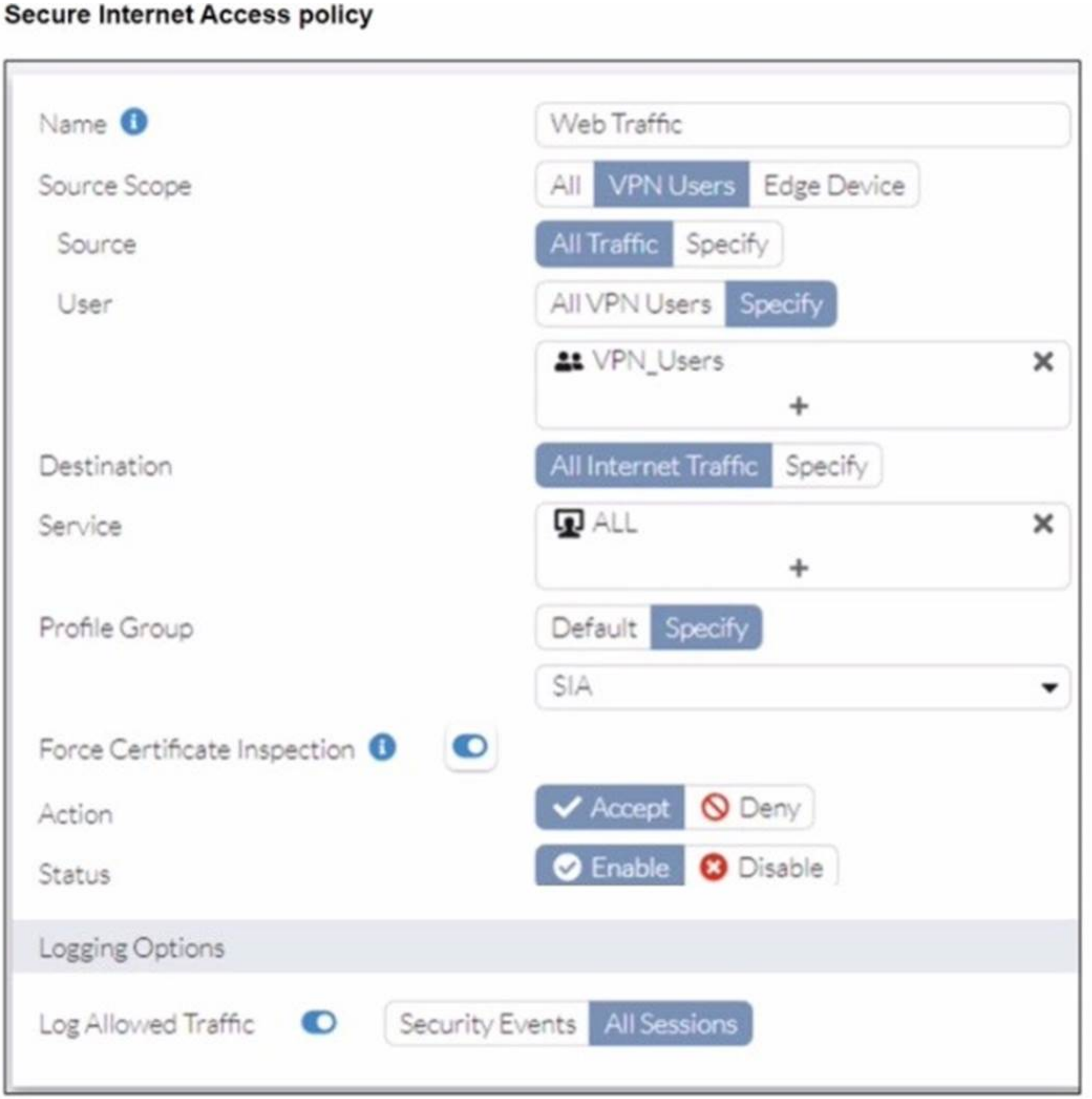
NEW QUESTION 5
Refer to the exhibits.

Web Filtering logs



Security Profile Group





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 6
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
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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