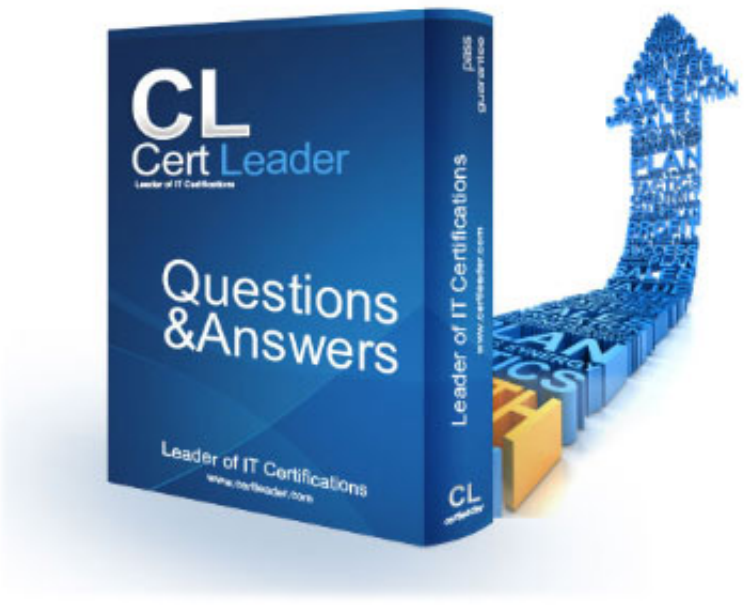
FCSS_SASE_AD-23 Dumps

FCSS FortiSASE 23 Administrator

https://www.certleader.com/FCSS_SASE_AD-23-dumps.html



NEW QUESTION 1
Which secure internet access (SIA) use case minimizes individual workstation or device setup, because you do not needto install FortiClient on endpoints or configure explicit web proxy settings on web browser-based end points?

A. SIA for inline-CASB users
B. SIA for agentless remote users
C. SIA for SSLVPN remote users
D. SIA for site-based remote users

Answer: B

Explanation:
The Secure Internet Access (SIA) use case that minimizes individual workstation or device setup is SIA for agentless remote users. This use case does not require installing FortiClient on endpoints or configuring explicit web proxy settings on web browser-based endpoints, making it the simplest and most efficient deployment.
? SIA for Agentless Remote Users:
? Minimized Setup:
References:
? FortiOS 7.2 Administration Guide: Details on different SIA deployment use cases and configurations.
? FortiSASE 23.2 Documentation: Explains how SIA for agentless remote users is implemented and the benefits it provides.

NEW QUESTION 2
Refer to the exhibit.

Daily report for application usage

FORTINET

User Productivity

Application Usage

The FortiGuard research team categorizes applications into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application control. FortiGuard maintains thousands of application sensors and can even perform deep application inspection. For example, IT managers can get unprecedented visibility into filenames sent to the cloud or the titles of videos being streamed.

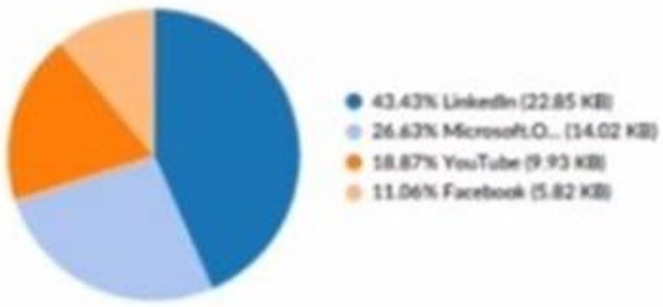
For application category details, see:
http://www.fortiguard.com/encyclopedia/application

App Categories

Unknown	41.81%
Web.Client	22.86%
Network.Service	15.14%
General.Interest	12.00%
Collaboration	6.23%
Update	1.50%
Video/Audio	0.21%
Social.Media	0.18%
Email	0.07%

With the proliferation of cloud-based computing, enterprises are increasingly reliant on third parties for infrastructure plumbing. Unfortunately for enterprises, this means that their information is only as secure as the cloud provider's security. In addition, it can often introduce redundancy (if services are already available internally) and increase costs (if not monitored properly).

Cloud Usage (SaaS)



IT managers are often unaware of how many cloud-based services are in use within their organization. Sometimes, these applications can be used to circumvent or even replace corporate infrastructure already available to users in lieu of ease of use. Unfortunately, a potential side effect of this is that your sensitive corporate information could be transferred to the cloud. Accordingly, your data could be exposed if the cloud provider's security infrastructure is breached.

The adoption of "infrastructure as a service" (IaaS) platforms is popular and can be very useful when compute resources are limited or have specialized requirements. That said, the effective outsourcing of your infrastructure must be well regulated to prevent misuse. The occasional auditing of IaaS applications can be a useful exercise not only for security purposes, but also to minimize organizational costs associated with pay per use models or recurring subscription fees.

Cloud Usage (IaaS)

No matching log data for this report

The daily report for application usage shows an unusually high number of unknown applications by category.
What are two possible explanations for this? (Choose two.)

A. Certificate inspection is not being used to scan application traffic.
B. The inline-CASB application control profile does not have application categories set to Monitor
C. Zero trust network access (ZTNA) tags are not being used to tag the correct users.
D. Deep inspection is not being used to scan traffic.

Answer: AD

Explanation:
The unusually high number of unknown applications by category in the daily report for application usage can be attributed to the following reasons:
? Certificate Inspection is not being used to scan application traffic:
? Deep Inspection is not being used to scan traffic:
References:
? FortiOS 7.2 Administration Guide: Details on certificate inspection and deep inspection configurations.
? FortiSASE 23.2 Documentation: Explains the importance of deep inspection and certificate inspection in accurate application identification.

NEW QUESTION 3
How does FortiSASE hide user information when viewing and analyzing logs?

A. By hashing data using Blowfish
B. By hashing data using salt
C. By encrypting data using Secure Hash Algorithm 256-bit (SHA-256)
D. By encrypting data using advanced encryption standard (AES)

Answer: B

Explanation:
FortiSASE hides user information when viewing and analyzing logs by hashing data using salt. This approach ensures that sensitive user information is obfuscated, enhancing privacy and security.
? Hashing Data with Salt:
? Security and Privacy:
References:
? FortiOS 7.2 Administration Guide: Provides information on log management and data protection techniques.
? FortiSASE 23.2 Documentation: Details on how FortiSASE implements data hashing and salting to secure user information in logs.

NEW QUESTION 4
Refer to the exhibits.

Managed Endpoints

Endpoint	VPN Username	Management Connection	ZTNA Tags (Simple)	FortiClient Version	Vulnerabilities Detected
Win10-Pro	user2@fortinettraining.lab	Online	FortiSASE-Compliant	7.0.10.0538	140
Win7-Pro	user1@fortinettraining.lab	Online	FortiSASE-Non-Compliant,FortiSASE-Compliant	7.0.8.0427	176

Secure Internet Access Policy

Create | Edit | Delete | Search

Name	Profile Group	Source	User	Destination	Action
Botnet Deny		all	All VPN Users	Botnet-C&C Server	Deny
Non-Compliant		FortiSASE-Non-Compliant	All VPN Users	All Internet Traffic	Deny
Web Traffic	SIA	FortiSASE-Compliant	VPN_Users	All Internet Traffic	Accept
Allow-All	Default		All VPN Users	All Internet Traffic	Accept
Implicit Deny		all	All VPN Users	All Internet Traffic	Deny

WiMO-Pro and Win7-Pro are endpoints from the same remote location. WiMO-Pro can
access the internet though FortiSASE, while Wm7-Pro can no longer access the internet Given the exhibits, which reason explains the outage on Wm7-Pro?

A. The Win7-Pro device posture has changed.
B. Win7-Pro cannot reach the FortiSASE SSL VPN gateway
C. The Win7-Pro FortiClient version does not match the FortiSASE endpoint requirement.
D. Win-7 Pro has exceeded the total vulnerability detected threshold.

Answer: D

Explanation:
Based on the provided exhibits, the reason why the Win7-Pro endpoint can no longer access the internet through FortiSASE is due to exceeding the total vulnerability detected threshold. This threshold is used to determine if a device is compliant with the security requirements to access the network.
? Endpoint Compliance:
? Vulnerability Threshold:
? Impact on Network Access:
References:
? FortiOS 7.2 Administration Guide: Provides information on endpoint compliance and vulnerability management.
? FortiSASE 23.2 Documentation: Explains how vulnerability thresholds are used to determine endpoint compliance and access control.

NEW QUESTION 5
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 6
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.

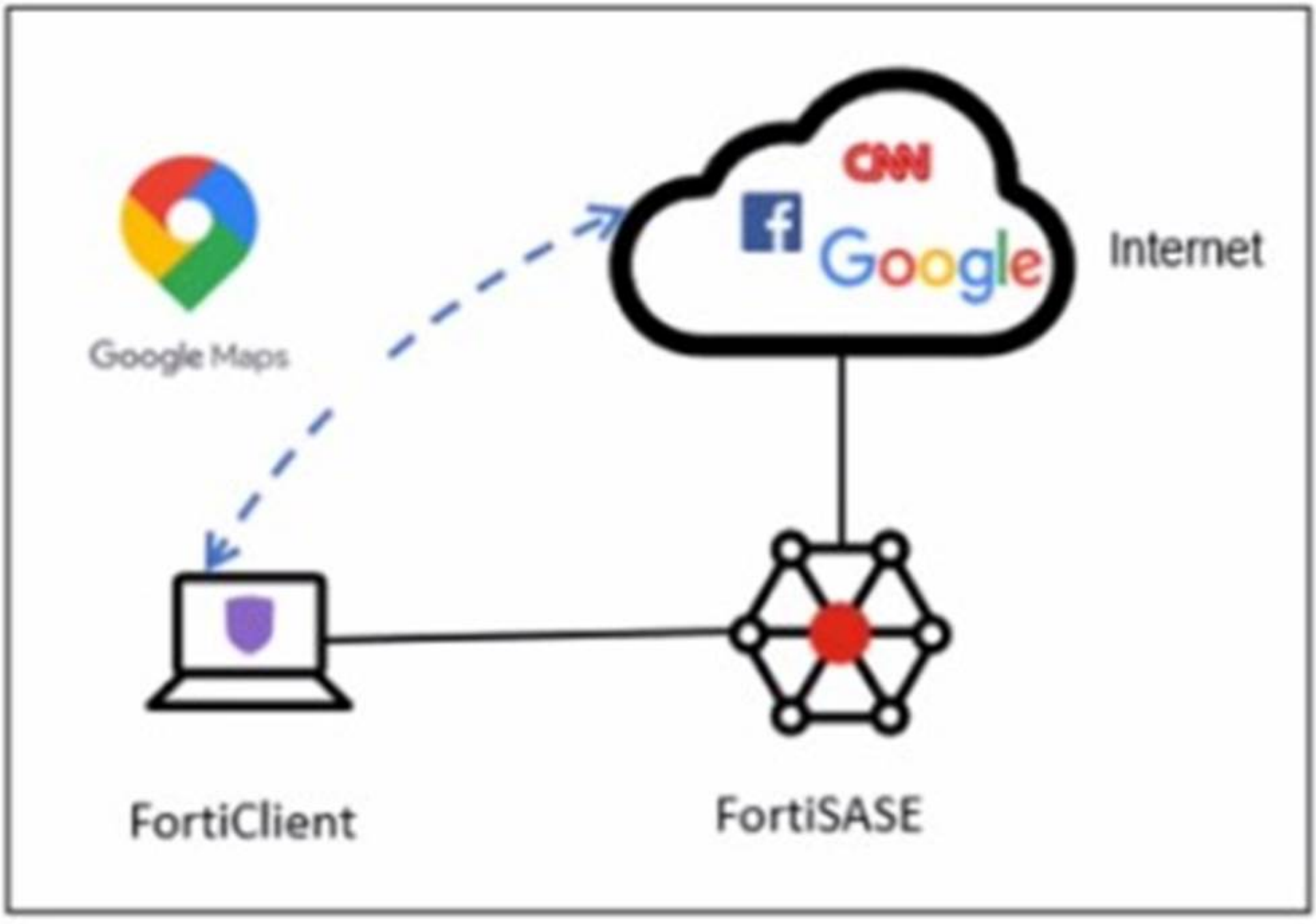
NEW QUESTION 7
Which two components are part of onboarding a secure web gateway (SWG) endpoint? (Choose two)

A. FortiSASE CA certificate
B. proxy auto-configuration (PAC) file
C. FortiSASE invitation code
D. FortiClient installer

Answer: AB

Explanation:
Onboarding a Secure Web Gateway (SWG) endpoint involves several components to
ensure secure and effective integration with FortiSASE. Two key components are the FortiSASE CA certificate and the proxy auto-configuration (PAC) file.
? FortiSASE CA Certificate:
? Proxy Auto-Configuration (PAC) File:
References:
? FortiOS 7.2 Administration Guide: Details on onboarding endpoints and configuring SWG.
? FortiSASE 23.2 Documentation: Explains the components required for integrating endpoints with FortiSASE and the process for deploying the CA certificate and PAC file.

NEW QUESTION 8
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?

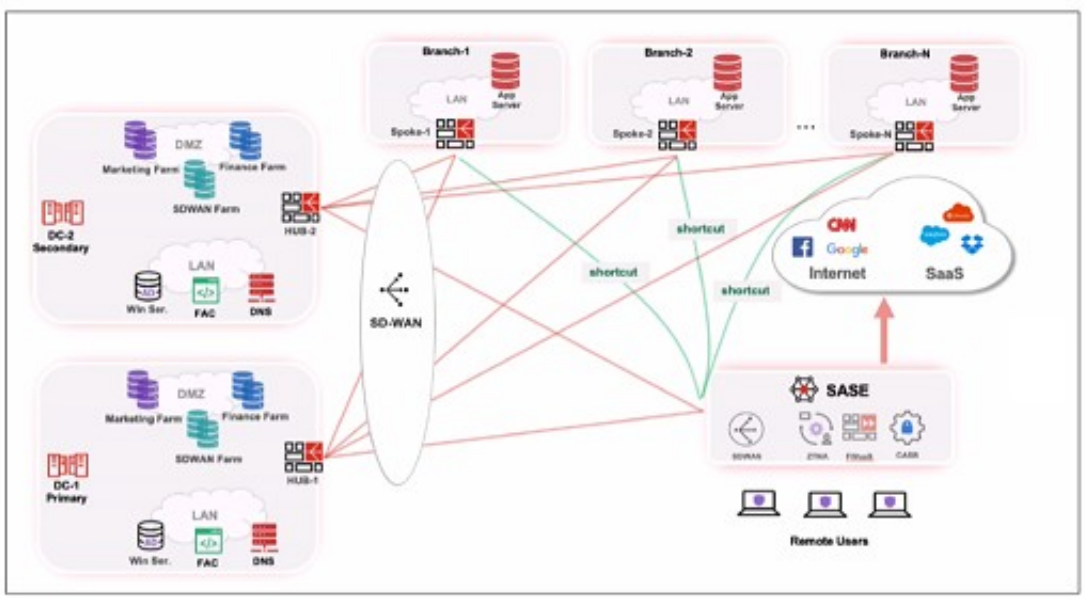
A. Exempt the Google Maps FQDN from the endpoint system proxy settings.
B. Configure a static route with the Google Maps FQDN on the endpoint to redirect traffic
C. Configure the Google Maps FQDN as a split tunneling destination on the FortiSASE endpoint profile.
D. Change the default DNS server configuration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

Answer: C

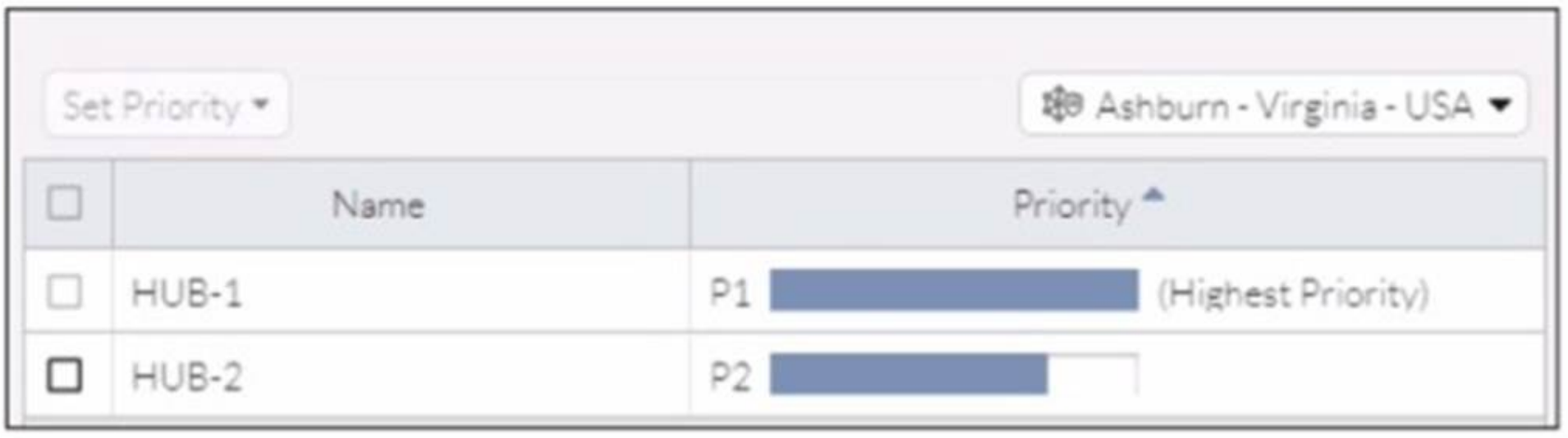
Explanation:
To meet the requirement of inspecting all endpoint internet traffic on FortiSASE while excluding Google Maps traffic from the FortiSASE VPN tunnel and redirecting it to the endpoint's physical interface, you should configure split tunneling. Split tunneling allows specific traffic to bypass 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 9
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?

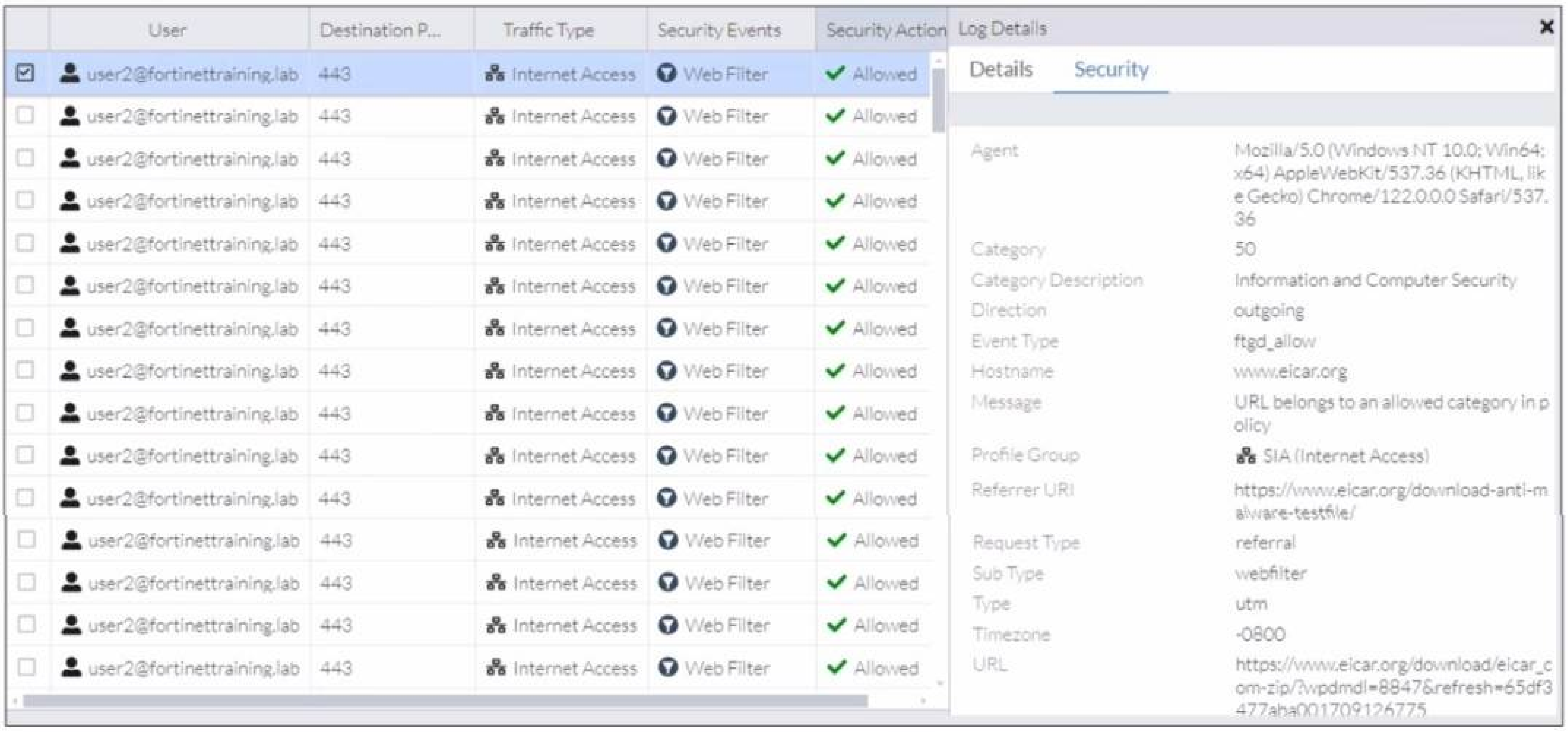
A. FortiSASE will use the SD-WAN capability and determine that traffic will be directed to HUB-2. which will then route traffic to Branch-2.
B. FortiSASE will use the AD VPN protocol and determine that traffic will be directed to Branch-2 directly, using a static route
C. FortiSASE will use the SD-WAN 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

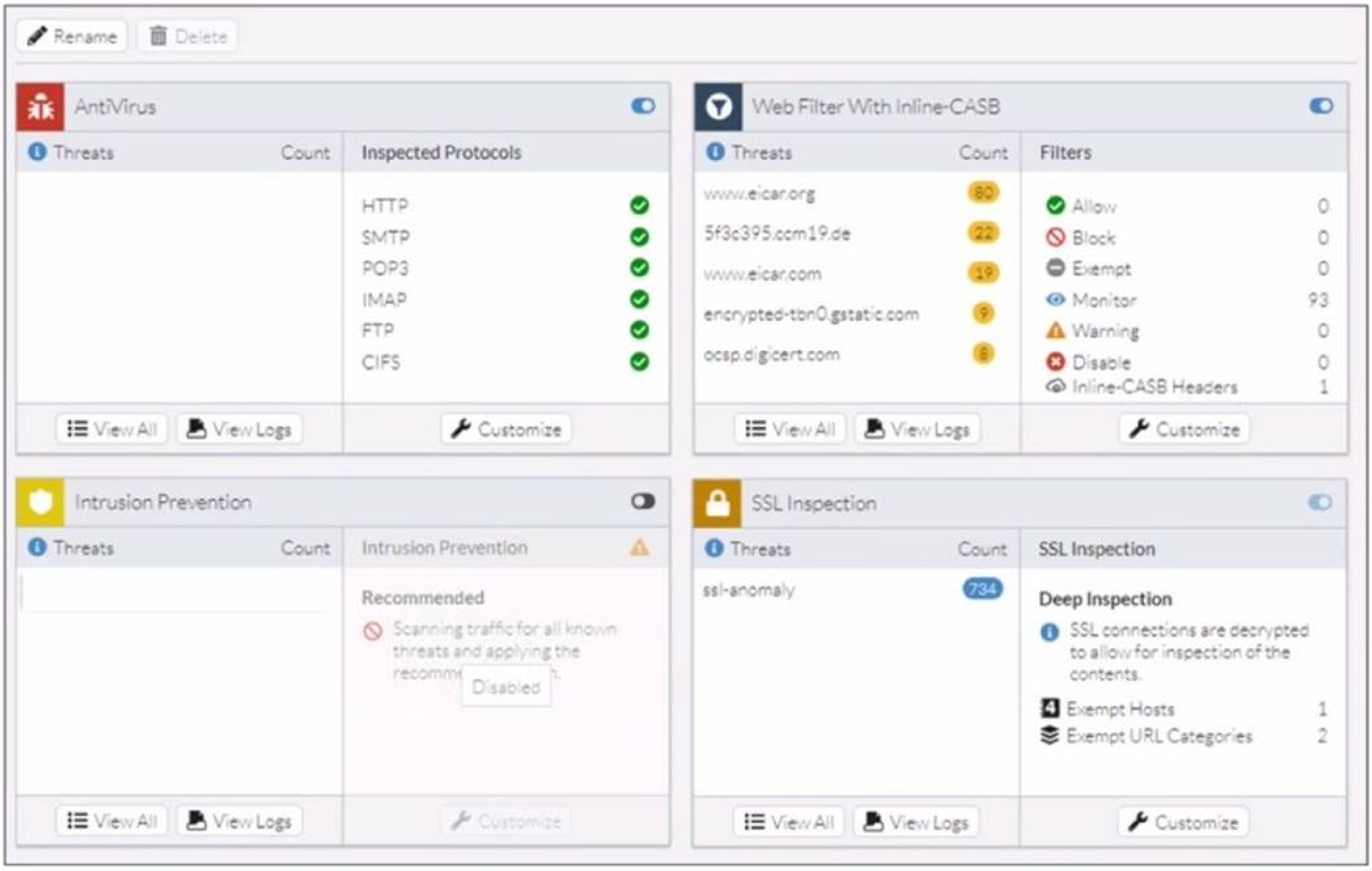
Explanation:
When remote users connected to FortiSASE require access to internal resources on Branch-2, the following process occurs:
? SD-WAN Capability:
? Traffic Routing Decision:
? Branch-2 Access:
References:
? FortiOS 7.2 Administration Guide: Details on SD-WAN configurations and priority settings.
? FortiSASE 23.2 Documentation: Explains how FortiSASE integrates with SD-WAN to route traffic based on defined priorities and performance metrics.

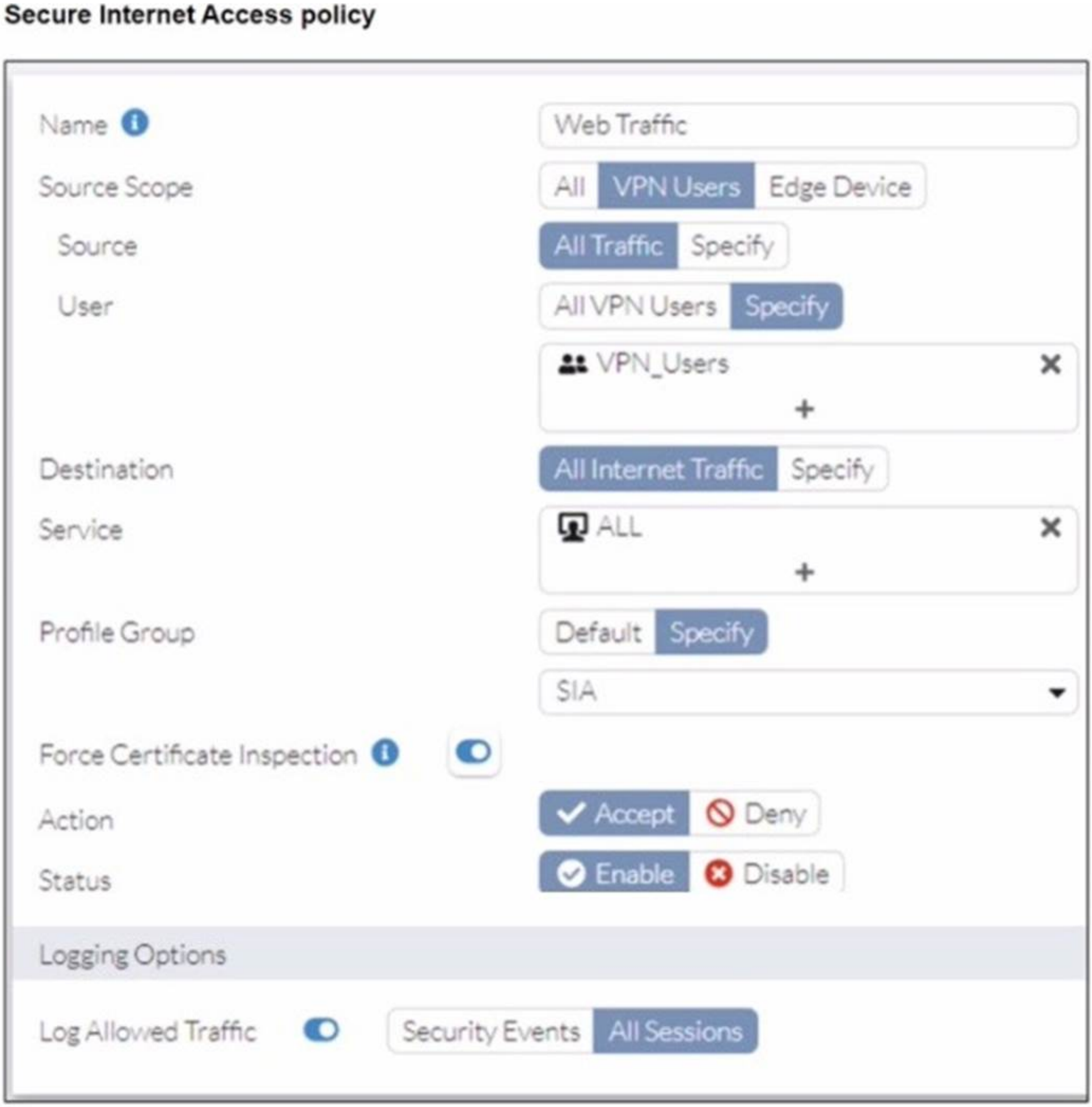
NEW QUESTION 10
Refer to the exhibits.

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 10
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.)

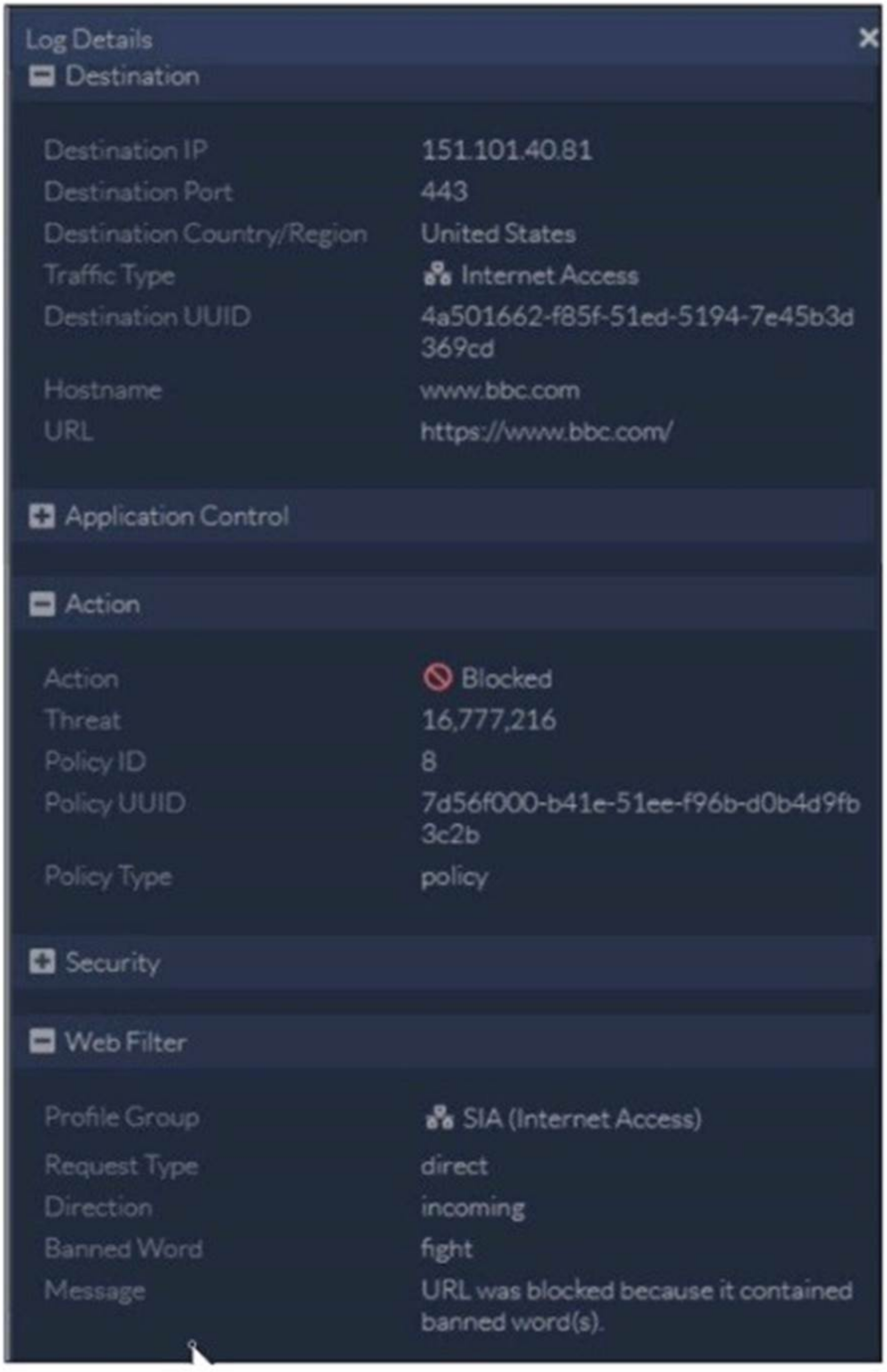
A. Add the FortiGate IP address in the secure private access configuration on FortiSASE.
B. Use the FortiClient EMS cloud connector on the corporate FortiGate to connect to FortiSASE
C. Register FortiGate and FortiSASE under the same FortiCloud account.
D. Authorize the corporate FortiGate on FortiSASE 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 15
Refer to the exhibit.

Security Logs



To allow access, which web tiller 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 URLhttps://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 19
Which role does FortiSASE play in supporting zero trust network access (ZTNA) principles9

A. It offers hardware-based firewalls for network segmentation.
B. It integrateswith software-defined network (SDN) solutions.
C. It can identify attributes on the endpoint for security posture check.
D. It enables VPN connections for remote employees.

Answer: C

Explanation:
FortiSASE supports zero trust network access (ZTNA) principles by identifying attributes on the endpoint for security posture checks. ZTNA principles require continuous verification of user and device credentials, as well as their security posture, before granting access to network resources.
? Security Posture Check:
? Zero Trust Network Access (ZTNA):
References:
? FortiOS 7.2 Administration Guide: Provides information on ZTNA and endpoint security posture checks.
? FortiSASE 23.2 Documentation: Details on how FortiSASE implements ZTNA
principles.

NEW QUESTION 23
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCSS_SASE_AD-23 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCSS_SASE_AD-23-dumps.html