Fortinet

Exam Questions FCSS_SASE_AD-24

FCSS - FortiSASE 24 Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

  All examinations will be up to date.

* 24/7 Quality Support

  We will provide service round the clock.

* 100% Pass Rate

  Our guarantee that you will pass the exam.

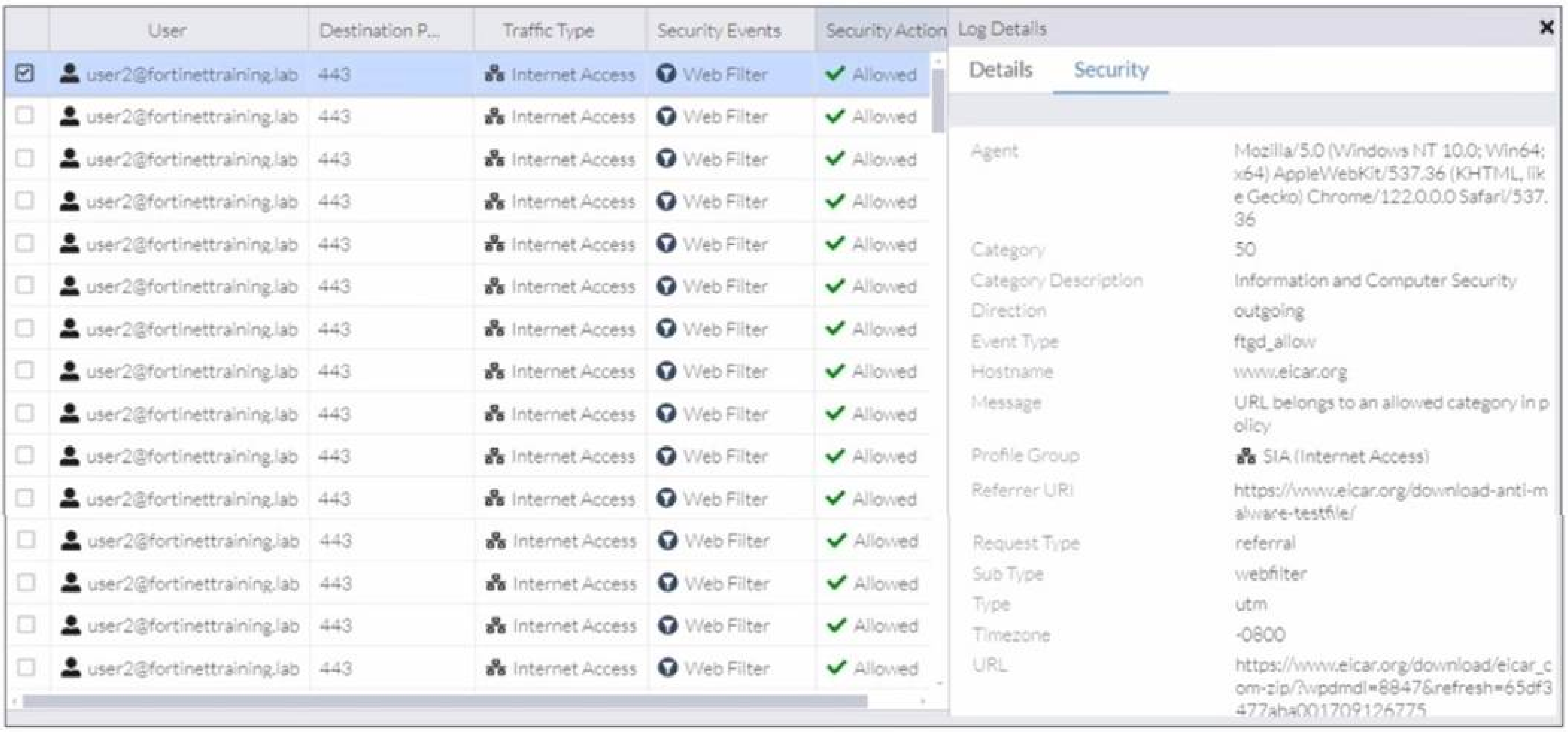
* Unique Gurantee

  If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

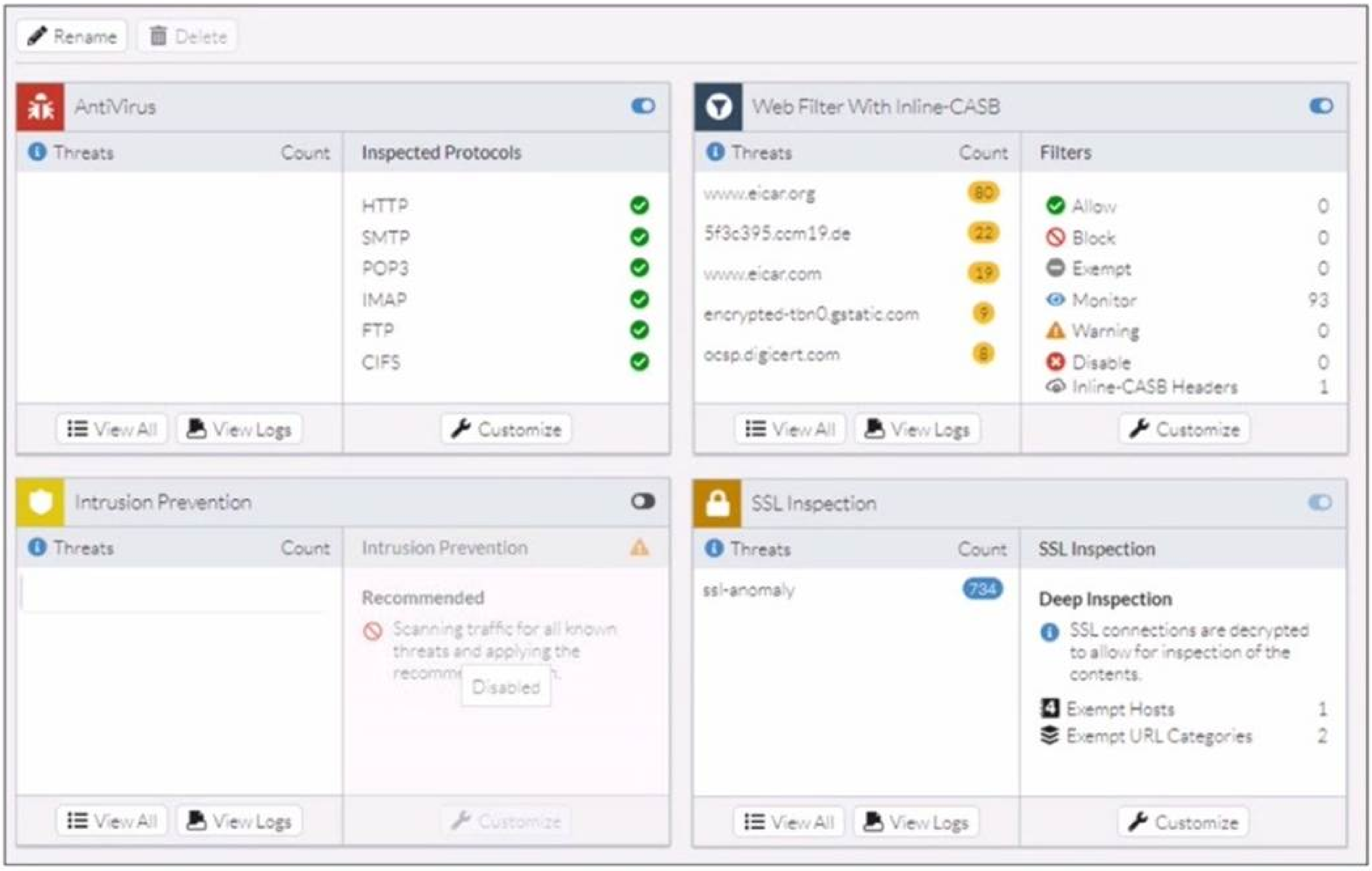
We recommend you to try the PREMIUM FCSS_SASE_AD-24 Dumps From Exambible
https://www.exambible.com/FCSS_SASE_AD-24-exam/ (43 Q&As)

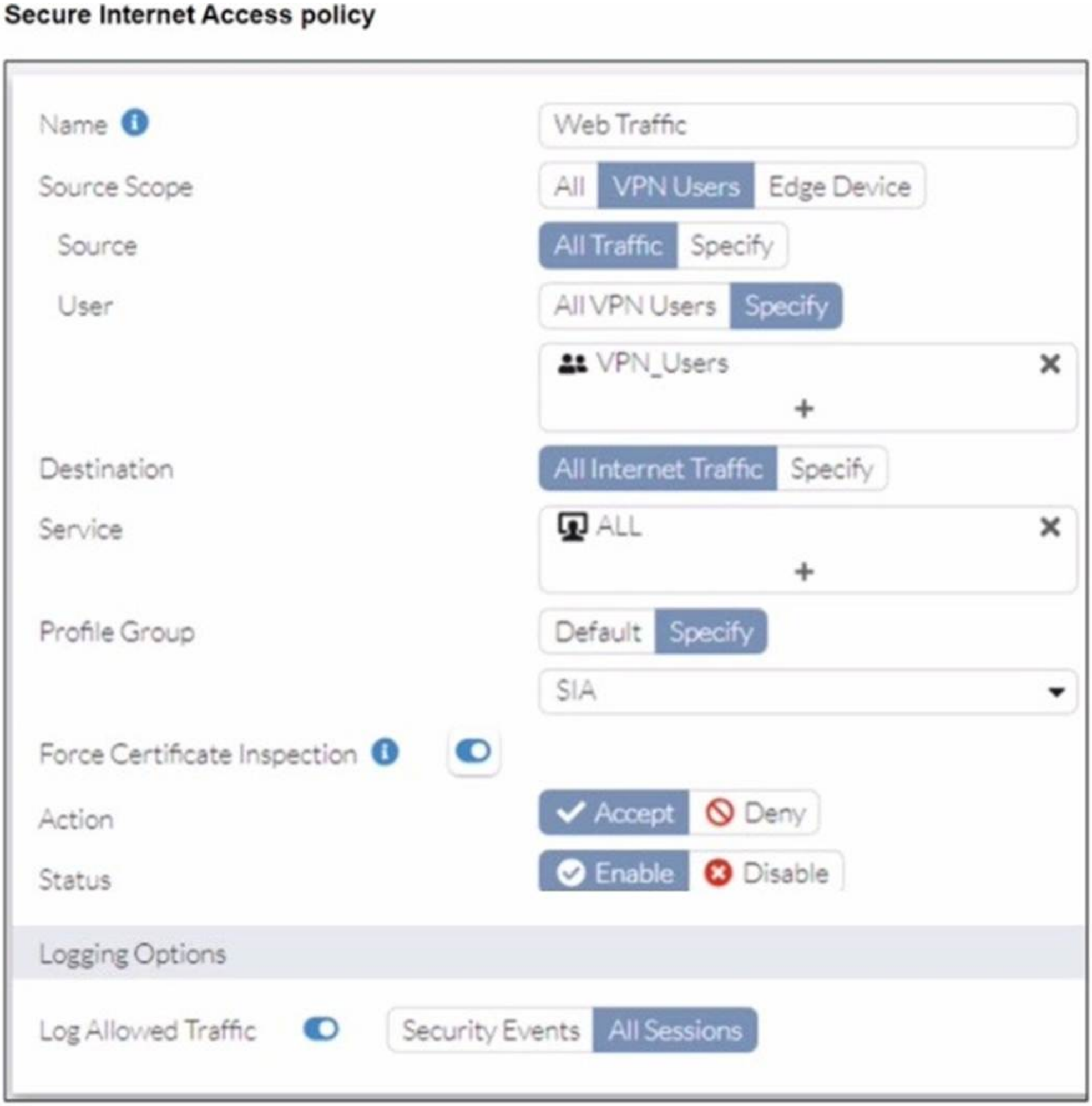
NEW QUESTION 1
Refer to the exhibits.

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: D

Explanation:
https://community.fortinet.com/t5/FortiSASE/Technical-Tip-Force-Certificate- Inspection-option-in-FortiSASE/ta-p/302617

NEW QUESTION 2
Which secure internet access (SIA) use case minimizes individual endpoint configuration?

A. Site-based remote user internet access
B. Agentless remote user internet access
C. SIA for SSL VPN remote users
D. SIA using ZTNA

Answer: B

Explanation:

Theagentless remote user internet accessuse case is designed to minimize individual endpoint configuration. In this scenario, FortiSASE provides secure internet access without requiring the installation of an agent on the endpoint device. This approach is particularly useful for environments with unmanaged devices or temporary users, as it eliminates the need for complex configurations on each endpoint. Instead, security policies are enforced at the network level, ensuring consistent protection without relying on endpoint-specific software.
Here??s why the other options are incorrect:
? A. Site-based remote user internet access:This use case involves securing internet access for users at a specific site or location, typically through a gateway or firewall. While it simplifies configuration for all users at that site, it does not specifically minimize individual endpoint configuration for remote users.
? C. SIA for SSL VPN remote users:SSL VPN requires users to connect to the corporate network via a client or browser-based interface. This approach often involves additional configuration on the endpoint, such as installing and configuring the SSL VPN client.
? D. SIA using ZTNA:Zero Trust Network Access (ZTNA) focuses on verifying the identity and posture of devices before granting access to resources. While ZTNA enhances security, it may require endpoint agents or posture checks, which involve some level of endpoint configuration.
References:
? Fortinet FCSS FortiSASE Documentation - Secure Internet Access (SIA) Use Cases
? FortiSASE Administration Guide - Agentless Remote User Access

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
Which event log subtype captures FortiSASE SSL VPN user creation?

A. Endpoint Events
B. VPN Events
C. User Events
D. Administrator Events

Answer: C

Explanation:
Theevent log subtypethat captures FortiSASE SSL VPN user creation is User Events. This subtype is specifically designed to log activities related to user management, such as creating, modifying, or deleting user accounts. When an SSL VPN user is created, it falls under this category because it involves adding a new user to the system.
Here??s why the other options are incorrect:
? A. Endpoint Events:These logs pertain to activities related to endpoint devices, such as device registration, compliance checks, or security posture assessments. SSL VPN user creation is unrelated to endpoint events.
? B. VPN Events:These logs capture activities related to VPN connections, such as session establishment, termination, or errors. While SSL VPN usage generates VPN events, the creation of a user account itself is not logged under this subtype.
? D. Administrator Events:These logs track actions performed by administrators, such as configuration changes or policy updates. While an administrator might create the SSL VPN user, the specific event of user creation is categorized under User Events, not Administrator Events.
References:
? Fortinet FCSS FortiSASE Documentation - Event Logging and Subtypes
? FortiSASE Administration Guide - Monitoring and Logging

NEW QUESTION 5
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 6
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 7
Which FortiSASE feature ensures least-privileged user access to all applications?

A. secure web gateway (SWG)
B. SD-WAN
C. zero trust network access (ZTNA)
D. thin branch SASE extension

Answer: C

Explanation:
Zero Trust Network Access (ZTNA) is the FortiSASE feature that ensures least-privileged user access to all applications. ZTNA operates on the principle of "never trust, always verify," providing secure access based on the identity of users and devices, regardless of their location.
? Zero Trust Network Access (ZTNA):
? Implementation:
References:
? FortiOS 7.2 Administration Guide: Provides detailed information on ZTNA and its role in ensuring least-privileged access.
? FortiSASE 23.2 Documentation: Explains the implementation and benefits of ZTNA within the FortiSASE environment.

NEW QUESTION 8
An organization needs to resolve internal hostnames using its internal rather than public DNS servers for remotely connected endpoints. Which two components must be configured on FortiSASE to achieve this? (Choose two.)

A. SSL deep inspection
B. Split DNS rules
C. Split tunnelling destinations
D. DNS filter

Answer: AB

Explanation:
To resolve internal hostnames using internal DNS servers for remotely connected endpoints, the following two components must be configured on FortiSASE:
? Split DNS Rules:

? Split Tunneling Destinations:
References:
? FortiOS 7.2 Administration Guide: Provides details on configuring split DNS and split tunneling for VPN clients.
? FortiSASE 23.2 Documentation: Explains the implementation and configuration of split DNS and split tunneling for securely resolving internal hostnames.

NEW QUESTION 10
.....

Relate Links

100% Pass Your FCSS_SASE_AD-24 Exam with Exambible Prep Materials

https://www.exambible.com/FCSS_SASE_AD-24-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/