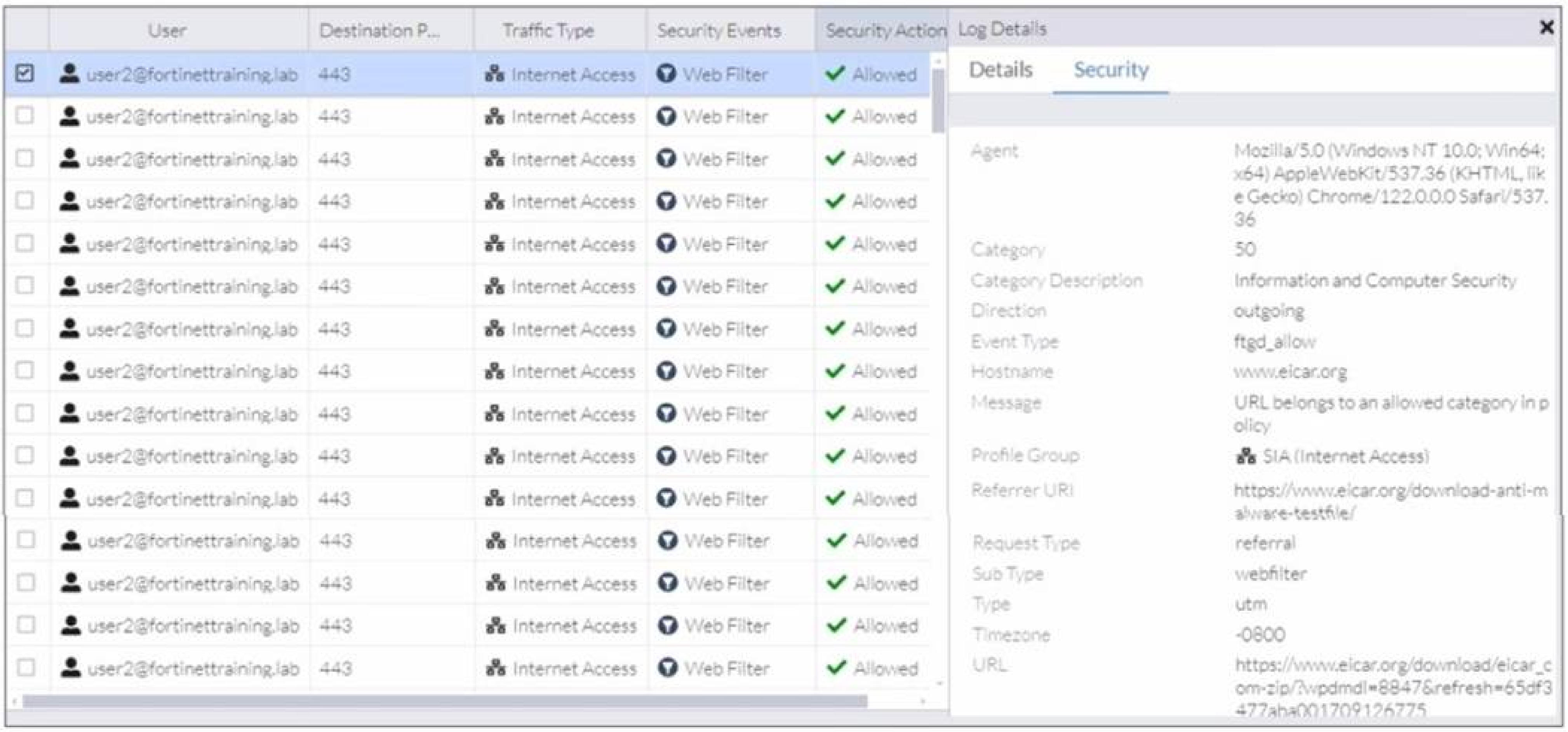
Fortinet

Exam Questions FCSS_SASE_AD-24

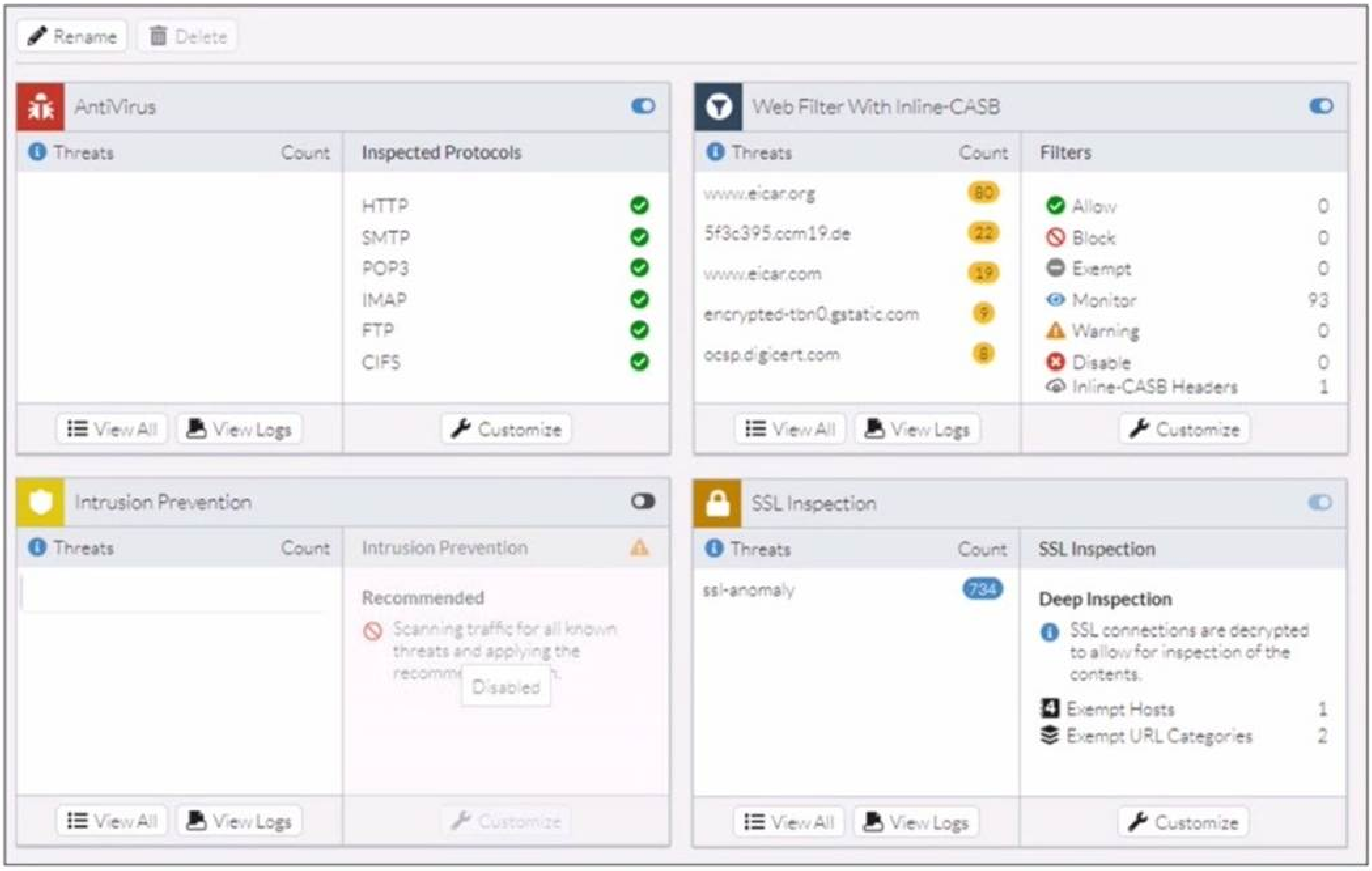
FCSS - FortiSASE 24 Administrator

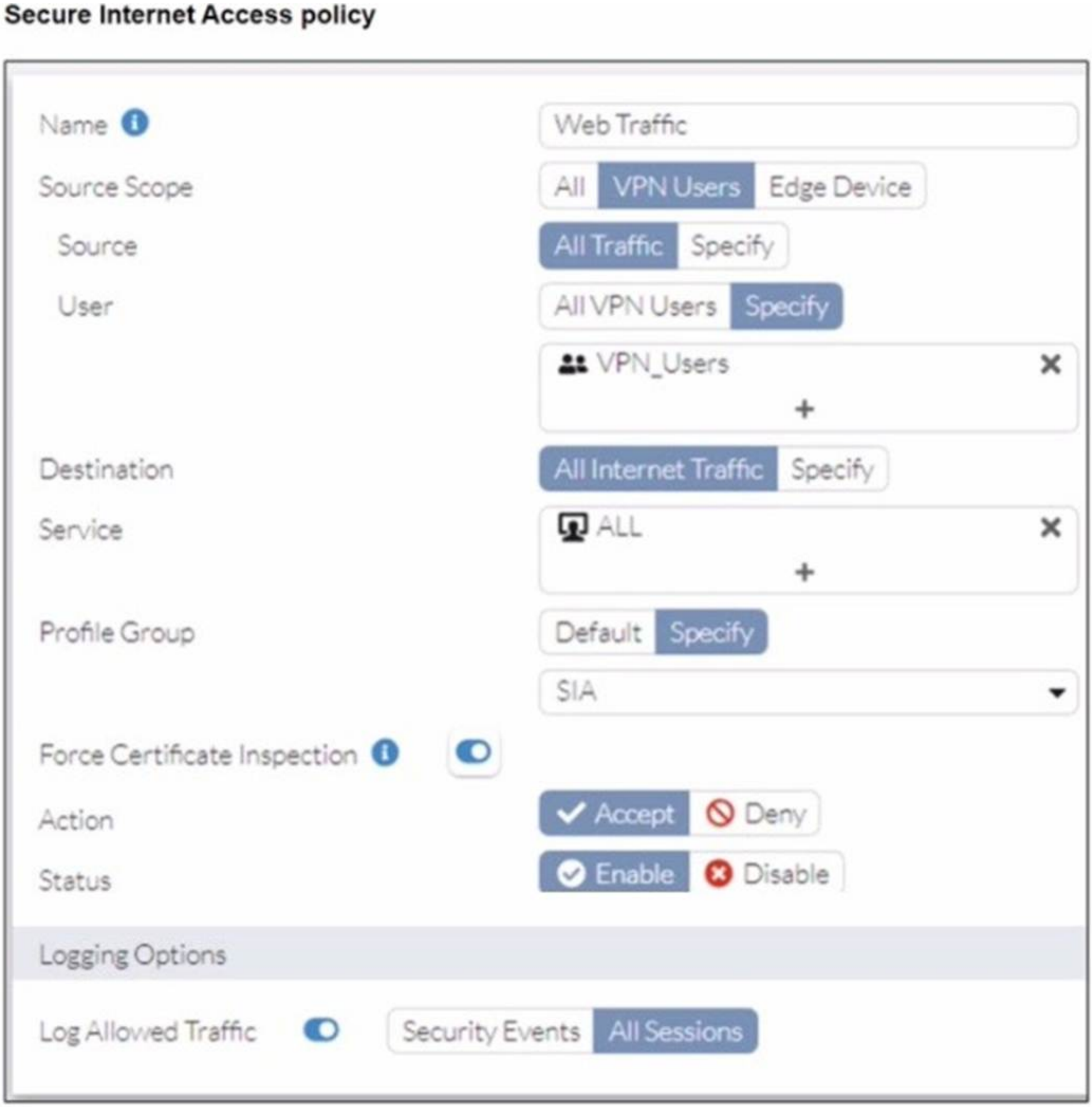
NEW QUESTION 1
Refer to the exhibits.

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 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: A

NEW QUESTION 5
Which two deployment methods are used to connect a FortiExtender as a FortiSASE LAN extension? (Choose two.)

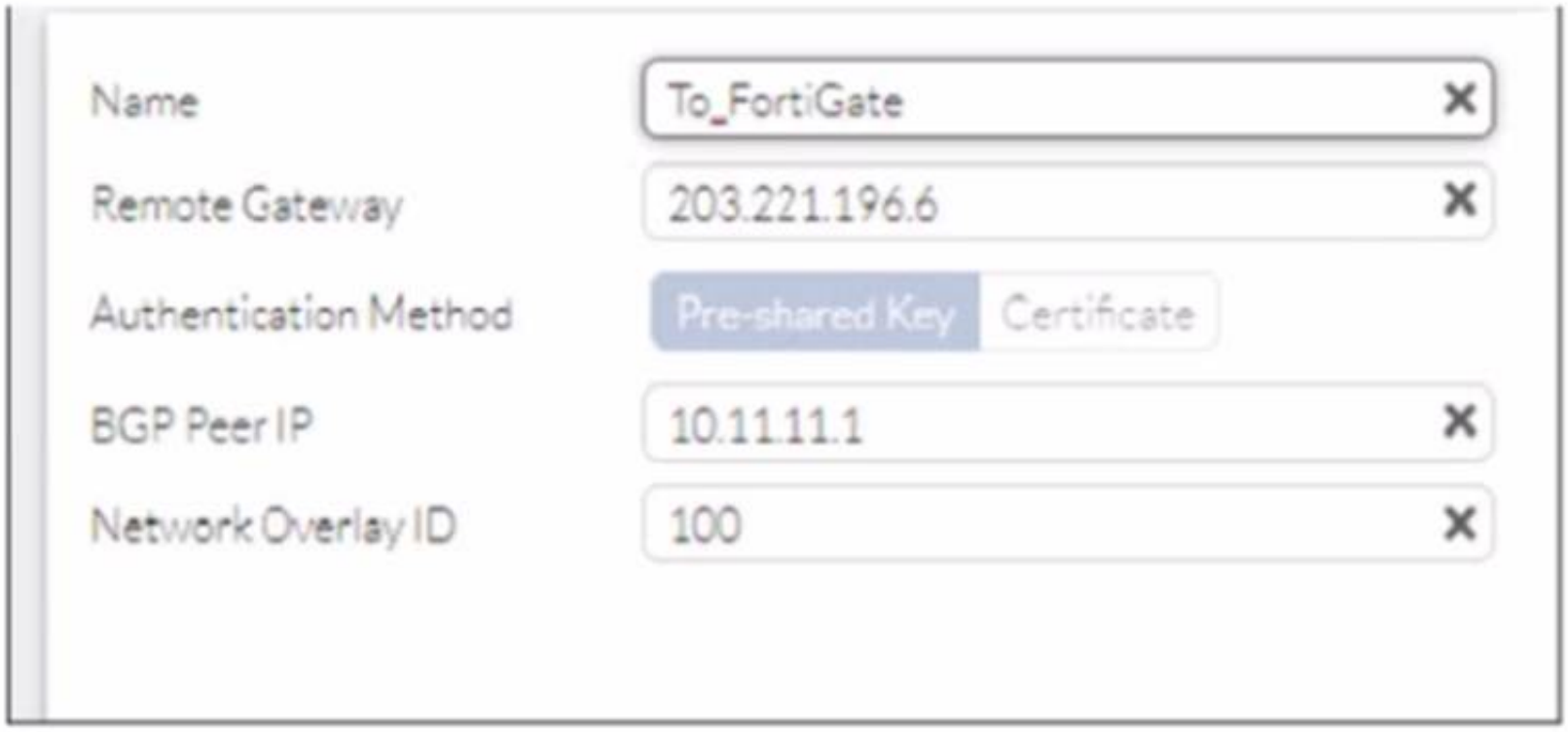
A. Connect FortiExtender to FortiSASE using FortiZTP
B. Enable Control and Provisioning Wireless Access Points (CAPWAP) access on the FortiSASE portal.
C. Enter the FortiSASE domain name in the FortiExtender GUI as a static discovery server
D. Configure an IPsec tunnel on FortiSASE to connect to FortiExtender.

Answer: AC

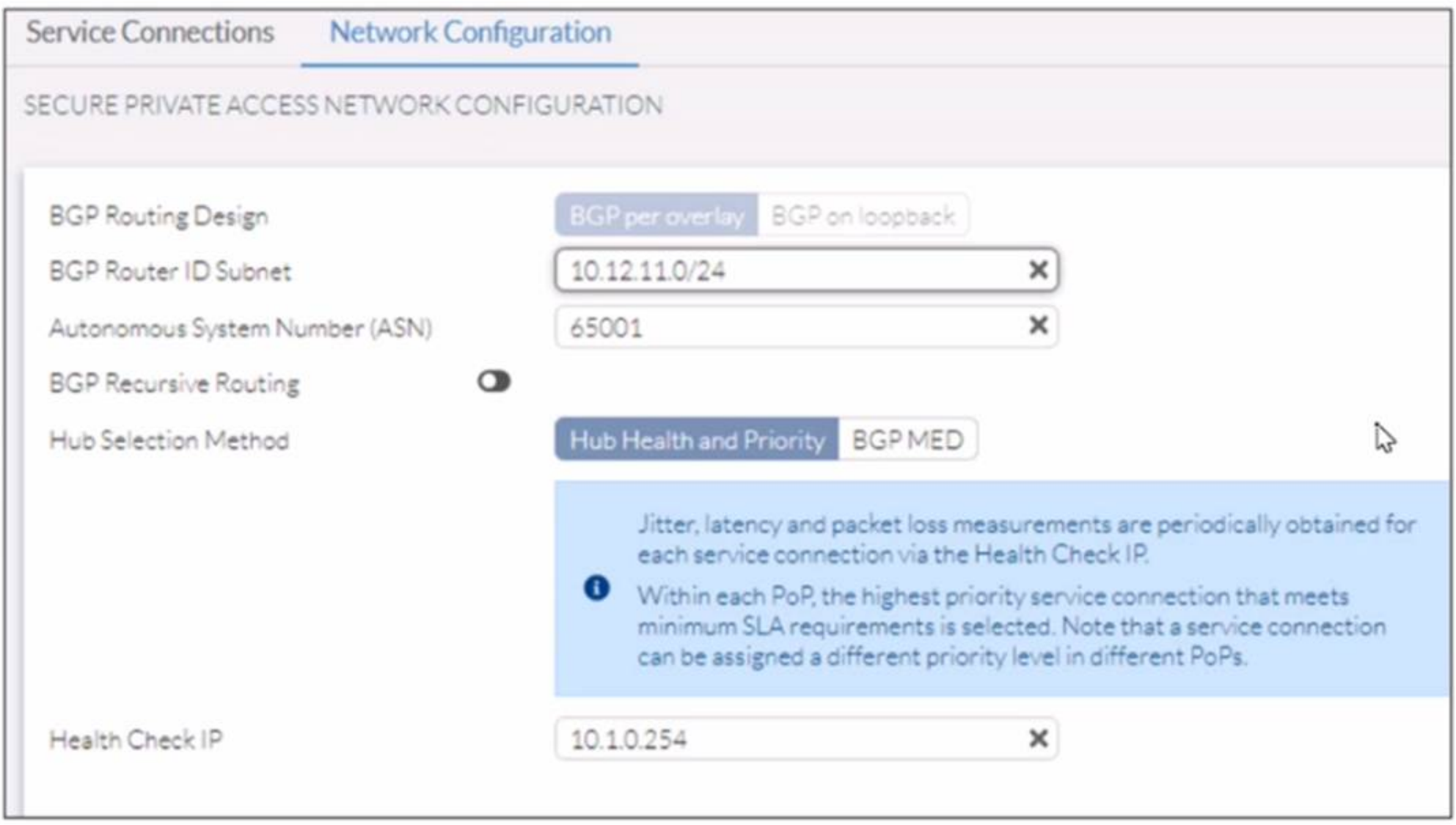
Explanation:
There are two deployment methods used to connect a FortiExtender as a FortiSASE LAN extension:
? Connect FortiExtender to FortiSASE using FortiZTP:
? Enter the FortiSASE domain name in the FortiExtender GUI as a static discovery server:
References:
? FortiOS 7.2 Administration Guide: Details on FortiExtender deployment methods and configurations.
? FortiSASE 23.2 Documentation: Explains how to connect and configure FortiExtender with FortiSASE using FortiZTP and static discovery.

NEW QUESTION 6
Refer to the exhibits.

Secure private access service connection



Secure private access network connection



Firewall policy configuration

```
config firewall policy
    edit 5
        set name "Spoke-to-Spoke"
        set uuid 4d949462-216b-51ee-03c7-d0662fdf9451
        set srcintf "To_SASE"
        set dstintf "To_SASE"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set comments "VPN: To_SASE (Created by VPN wizard)"
    next
    edit 6
        set name "Lo-BGP-HC"
        set uuid f5a12c92-216b-51ee-4802-80cd013d6acf
        set srcintf "To_SASE"
        set dstintf "SASE_Health"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
    edit 9
        set name "Spoke-to-Hub"
        set uuid 617b81ee-cc64-51ee-8da6-6cdff3ca2cca
        set srcintf "To_SASE"
        set dstintf "internal3"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

IPsec VPN configuration

```
# show vpn ipsec phase1-interface To_SASE
 config vpn ipsec phase1-interface
   edit "To_SASE"
        set type dynamic
        set interface "wan1"
        set peertype any
        set net-device disable
        set mode-cfg enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set comments "VPN: To_SASE (Created by VPN wizard)"
        set wizard-type hub-fortigate-auto-discovery
        set auto-discovery-sender enable
        set ipv4-start-ip 10.11.11.10
        set ipv4-end-ip 10.11.11.200
        set ipv4-netmask 255.255.255.0
        set unity-support disable
        set psksecret ENC Sbl0igpvIFFYSpRZ/hyxQVUXv9NZm7uqltD9v+BViPd+7RWizmUA3ZINn0zbsxq70F
  iYkPLkxaNwIo7VLIipkye1xt84NAwEfm5jTqqf1dMj/phYvBI3hzU0yXg==
    next
 end

# show vpn ipsec phase2-interface To_SASE
config vpn ipsec phase2-interface
    edit "To_SASE"
        set phase1name "To_SASE"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
        set comments "VPN: To_SASE (Created by VPN wizard)"
    next
 end
```

BGP protocol configuration

```
#config router bgp
      set as 65001
      set router-id 10.1.0.254
      config neighbor
          edit "10.10.1.3"
              set advertisement-interval 1
              set ebgp-enforce-multihop enable
              set link-down-failover enable
              set remote-as 65001
              set route-reflector-client enable
          next
      end
      config neighbor-group
          edit "To_SASE"
              set capability-graceful-restart enable
              set link-down-failover enable
              set next-hop-self enable
              set interface "To_SASE"
              set remote-as 65001
              set additional-path both
              set adv-additional-path 4
              set route-reflector-client enable
          next
      end
      config neighbor-range
          edit 1
              set prefix 10.11.11.0 255.255.255.0
              set neighbor-group "To_SASE"
          next
      end
      config network
          edit 1
              set prefix 10.190.190.0 255.255.255.0
          next
      end
```

A FortiSASE administrator is trying to configure FortiSASE as a spoke to a FortiGate hub. The VPN tunnel does not establish
Based on the provided configuration, what configuration needs to be modified to bring the tunnel up?

A. NAT needs to be enabled in the Spoke-to-Hub firewall policy.
B. The BGP router ID needs to match on the hub and FortiSASE.
C. FortiSASE spoke devices do not support mode config.
D. The hub needs IKEv2 enabled in the IPsec phase 1 settings.

Answer: D

NEW QUESTION 7
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 8
Which statement best describes the Digital Experience Monitor (DEM) feature on FortiSASE?

A. It provides end-to-end network visibility from all the FortiSASE security PoPs to a specific SaaS application.
B. It can be used to request a detailed analysis of the endpoint from the FortiGuard team.
C. It requires a separate DEM agent to be downloaded from the FortiSASE portal and installed on the endpoint.
D. It can help IT and security teams ensure consistent security monitoring for remote users.

Answer: A

Explanation:
TheDigital Experience Monitor (DEM)feature in FortiSASE is designed to provideend-to-end network visibilityby monitoring the performance and health of connections between FortiSASE security Points of Presence (PoPs) and specific SaaS applications. This ensures that administrators can identify and troubleshoot issues related to latency, jitter, packet loss, and other network performance metrics that could impact user experience when accessing cloud-based services.
Here??s why the other options are incorrect:
? B. It can be used to request a detailed analysis of the endpoint from the FortiGuard team:This is incorrect because DEM focuses on network performance monitoring, not endpoint analysis. Endpoint analysis would typically involve tools like FortiClient or FortiEDR, not DEM.
? C. It requires a separate DEM agent to be downloaded from the FortiSASE portal and installed on the endpoint:This is incorrect because DEM operates at the network level and does not require an additional agent to be installed on endpoints.
? D. It can help IT and security teams ensure consistent security monitoring for remote users:While DEM indirectly supports security by ensuring optimal network performance, its primary purpose is to monitor and improve the digital experience rather than enforce security policies.
References:
? Fortinet FCSS FortiSASE Documentation - Digital Experience Monitoring Overview
? FortiSASE Administration Guide - Configuring DEM
==========

NEW QUESTION 9
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
.....

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-24 Practice Exam Features:

* FCSS_SASE_AD-24 Questions and Answers Updated Frequently

* FCSS_SASE_AD-24 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_SASE_AD-24 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_SASE_AD-24 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year