Fortinet

Exam Questions FCSS_SASE_AD-23

FCSS FortiSASE 23 Administrator

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
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 3
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.

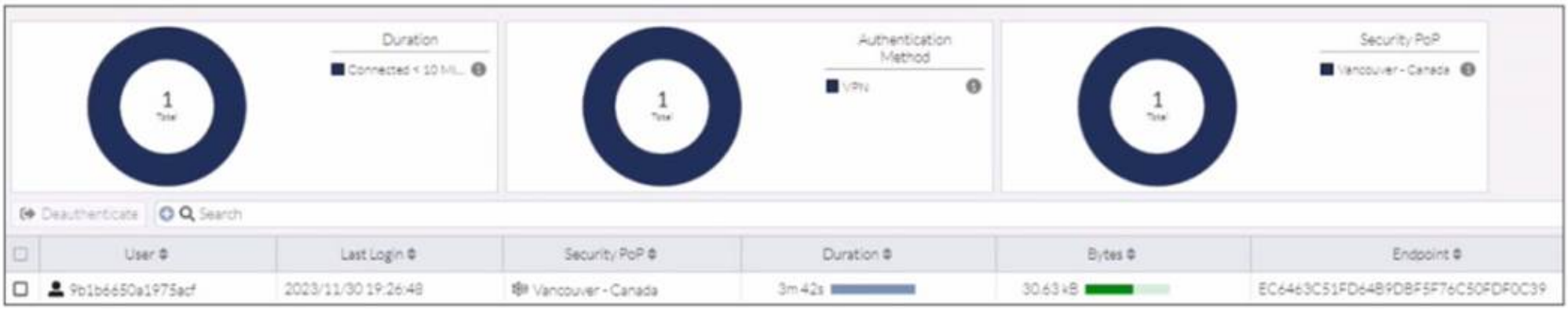
NEW QUESTION 4
Which two components are part of onboarding a secure web gateway (SWG) endpoint? (Choose two)

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 5
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 6
When you configure FortiSASE Secure Private Access (SPA) with SD-WAN integration, you must establish a routing adjacency between FortiSASE and the FortiGate SD-WAN hub. Which routing protocol must you use?

A. BGP
B. IS-IS
C. OSPF
D. EIGRP

Answer: A

Explanation:
When configuring FortiSASE Secure Private Access (SPA) with SD-WAN integration, establishing a routing adjacency between FortiSASE and the FortiGate SD-WAN hub requires the use of the Border Gateway Protocol (BGP).
? BGP (Border Gateway Protocol):
? Routing Adjacency:
References:
? FortiOS 7.2 Administration Guide: Provides information on configuring BGP for SD-WAN integration.
? FortiSASE 23.2 Documentation: Details on setting up routing adjacencies using BGP for Secure Private Access with SD-WAN.

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 wants to block all video and audio application traffic but grant access to videos from CNN Which application override action must you configure in the Application Control with Inline-CASB?

A. Allow
B. Pass
C. Permit

D. Exempt

Answer: D

Explanation:
? Application Control Configuration:
? Blocking Video and Audio Applications:
? Granting Access to Specific Videos (CNN):
? Configuration Steps:
References:
? FortiOS 7.2 Administration Guide: Detailed steps on configuring Application Control and Inline-CASB.
? Fortinet Training Institute: Provides scenarios and examples of using Application Control with Inline-CASB for specific use cases.

NEW QUESTION 9
What are two advantages of using zero-trust tags? (Choose two.)

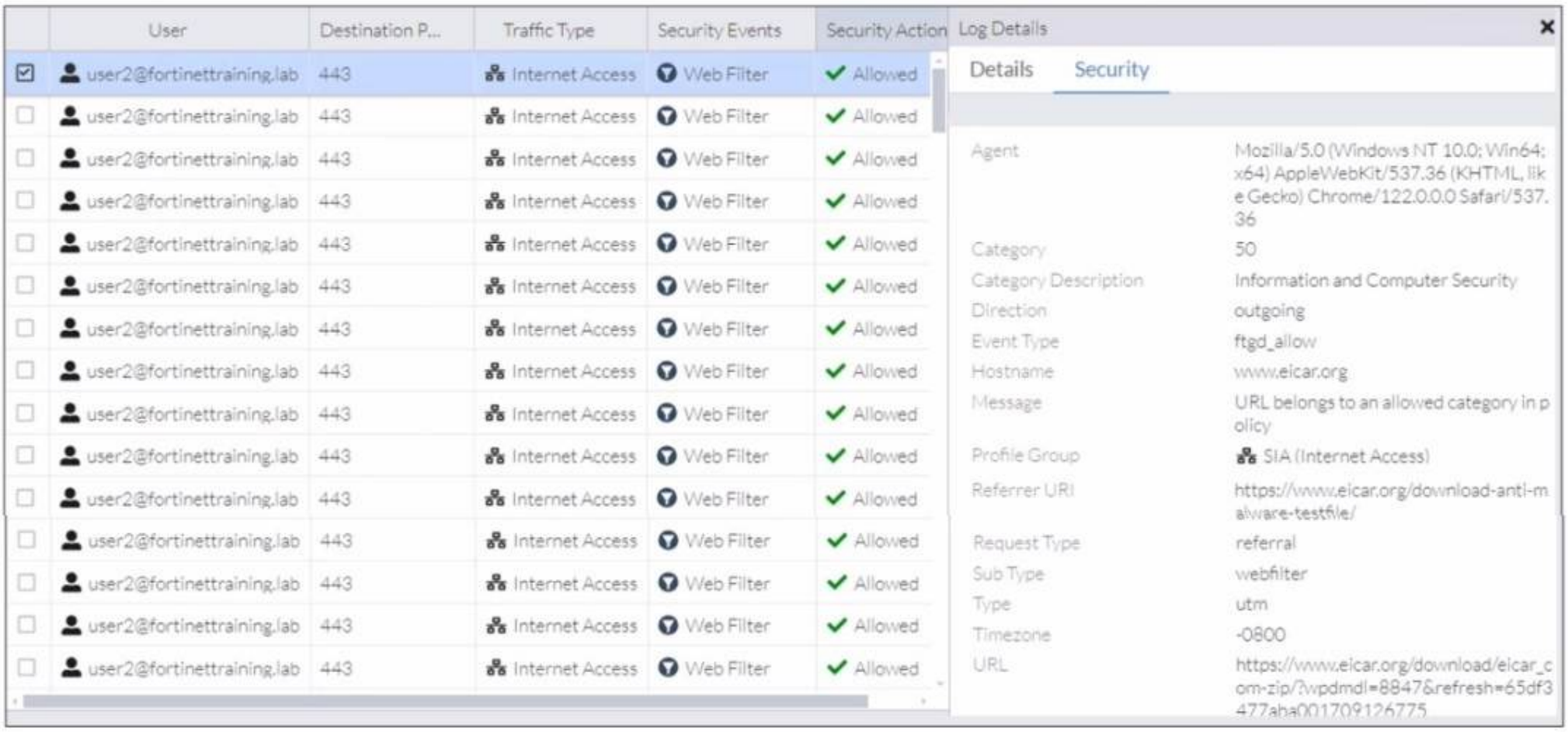
A. Zero-trust tags can be used to allow or deny access to network resources
B. Zero-trust tags can determine the security posture of an endpoint.
C. Zero-trust tags can be used to create multiple endpoint profiles which can be applied to different endpoints
D. Zero-trust tags can be used to allow secure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

Answer: AB

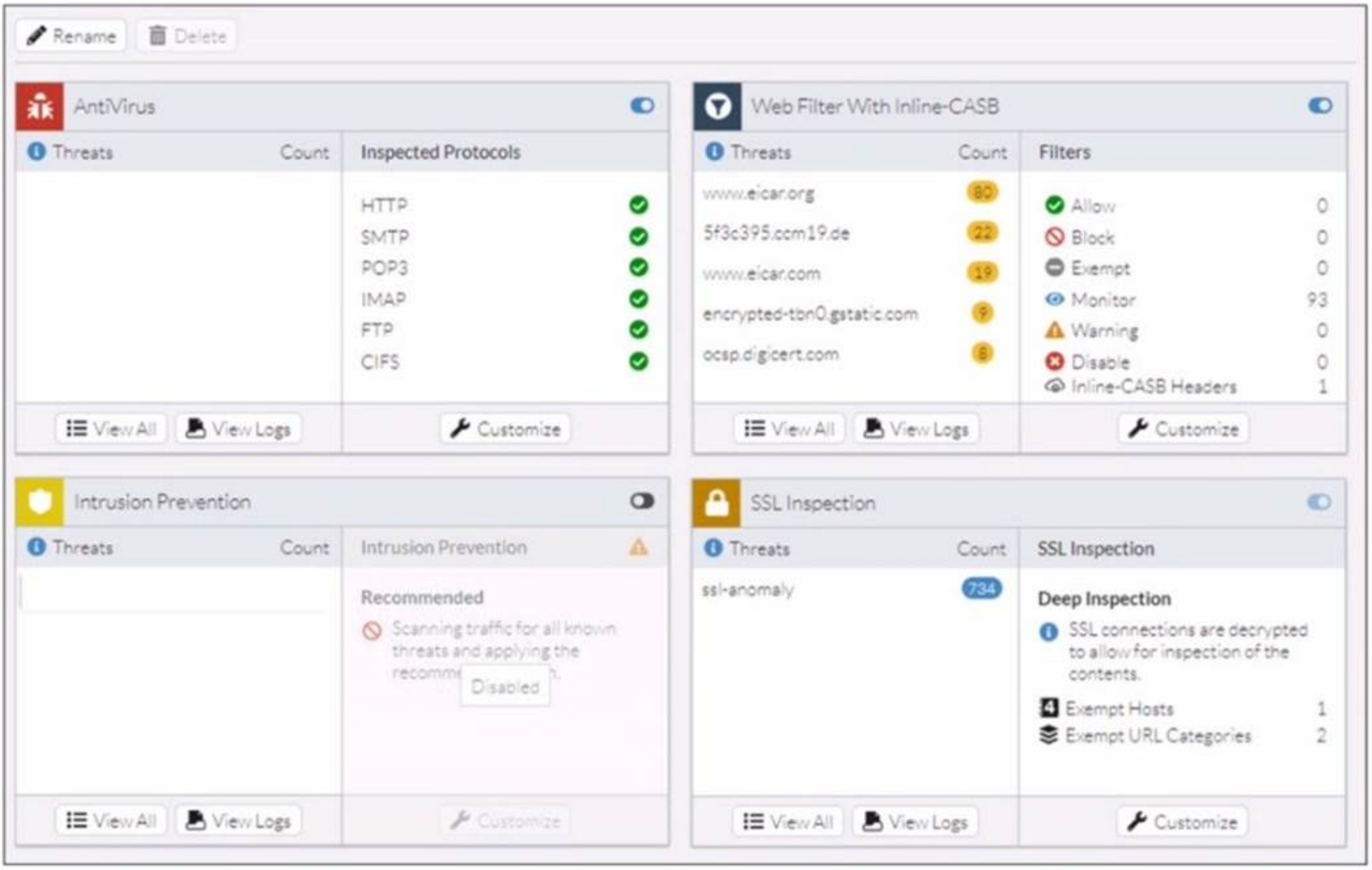
Explanation:
Zero-trust tags are critical in implementing zero-trust network access (ZTNA) policies. Here are the two key advantages of using zero-trust tags:
? Access Control (Allow or Deny):
? Determining Security Posture:
References:
? FortiOS 7.2 Administration Guide: Provides detailed information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

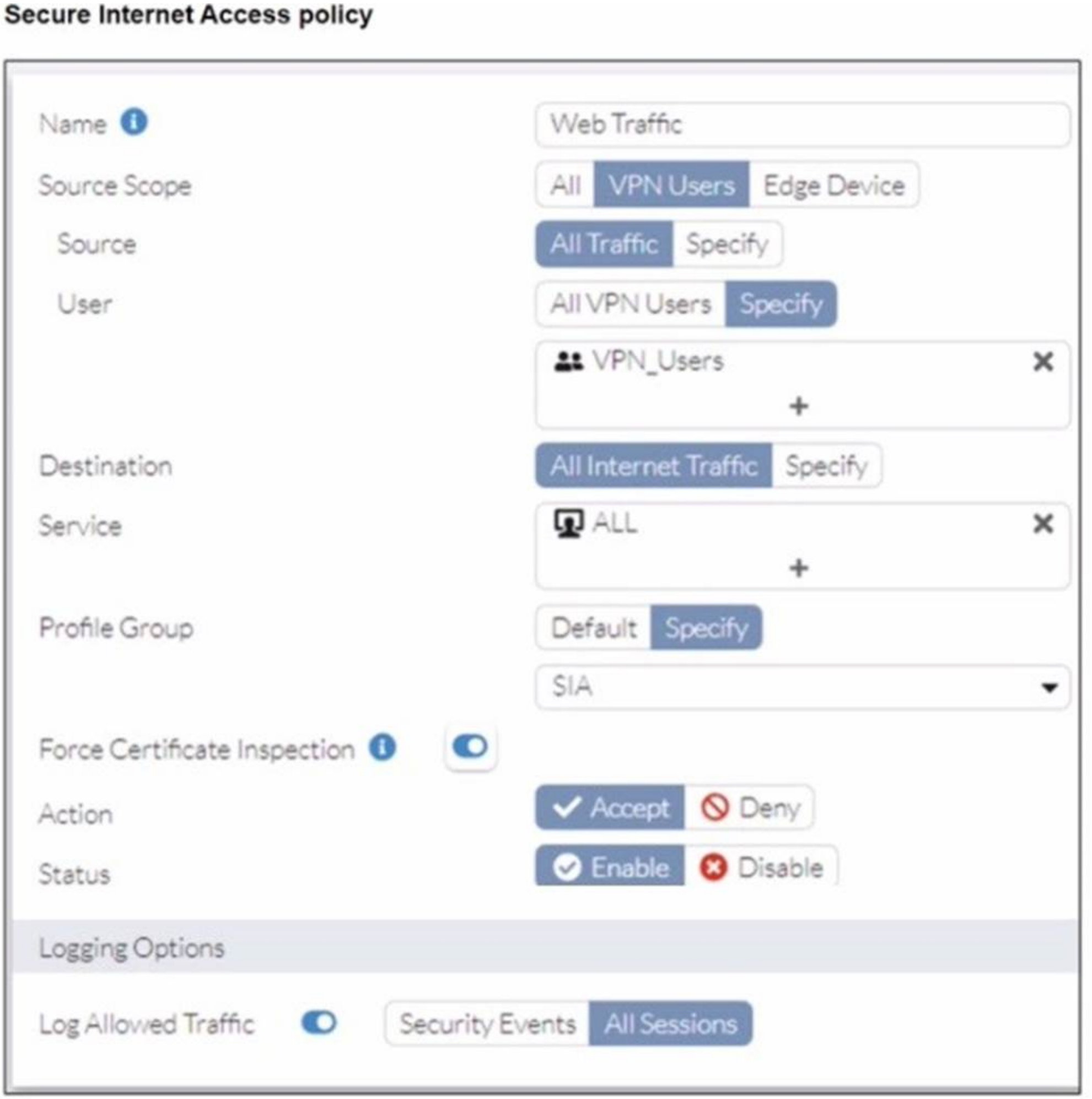
NEW QUESTION 10
Refer to the exhibits.

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?

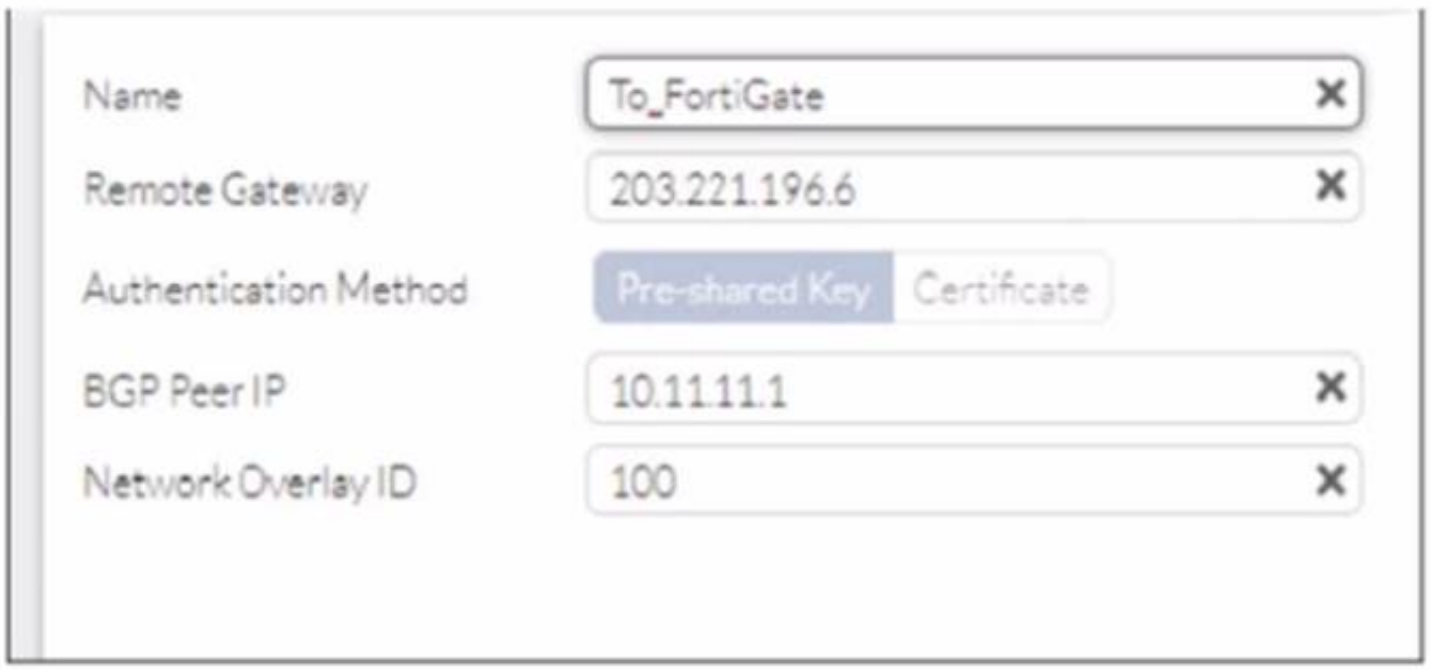
A. Web filter is allowing the traffic.
B. IPS is disabled in the security profile group.
C. The HTTPS protocol is not enabled in the antivirus profile.
D. Force certificate inspection is enabled in the policy.

Answer: A

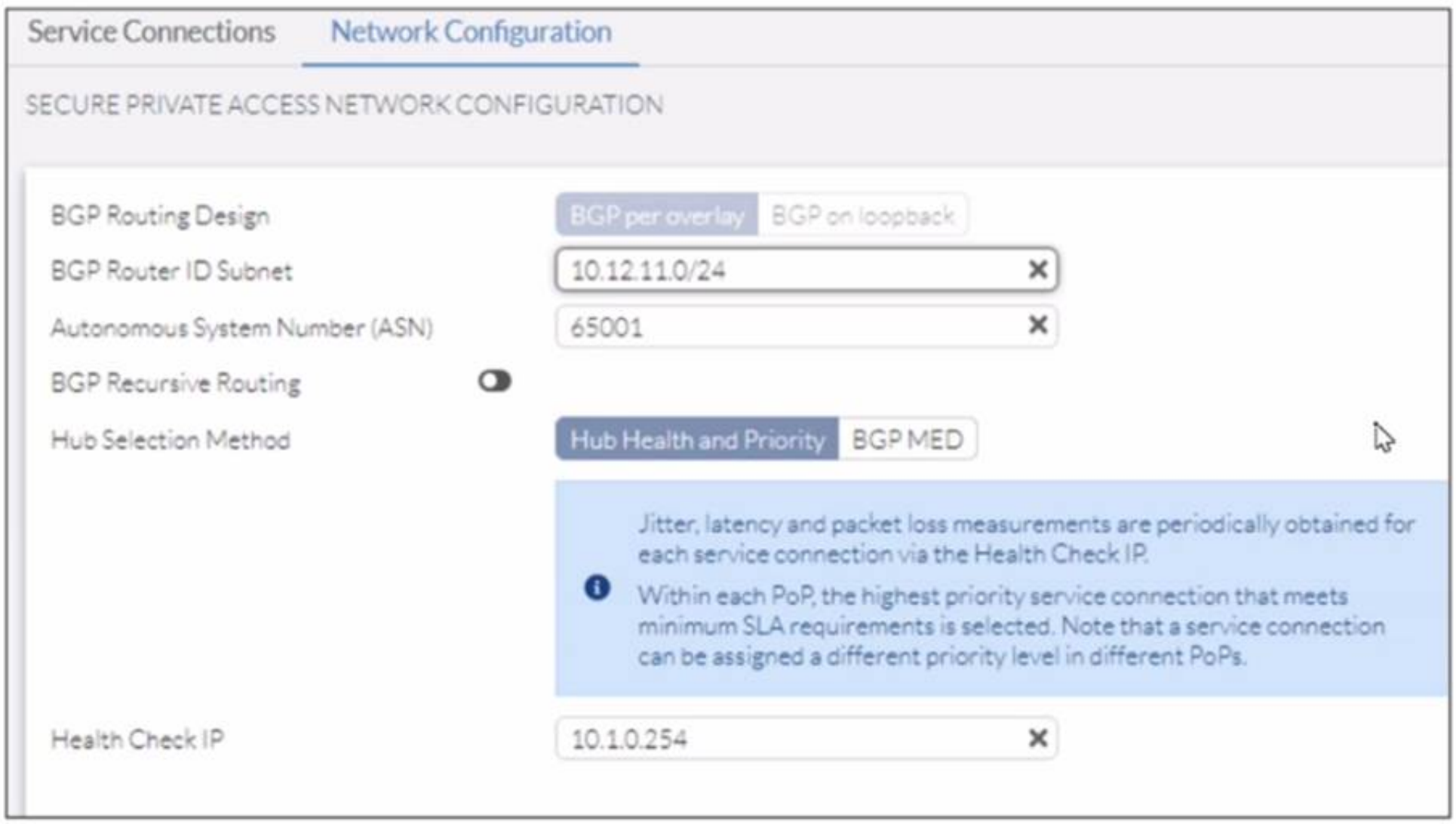
Explanation:
? Web Filtering Logs Analysis:
? Security Profile Group Configuration:
? Antivirus Profile Configuration:
? Policy Configuration:
References:
? FortiGate Security 7.2 Study Guide: Provides details on the precedence of web filtering over antivirus in security profiles.
? Fortinet Knowledge Base: Detailed explanation of web filtering and antivirus
profiles interaction.

NEW QUESTION 10
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 SblOigpvIFFYSpRZ/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?

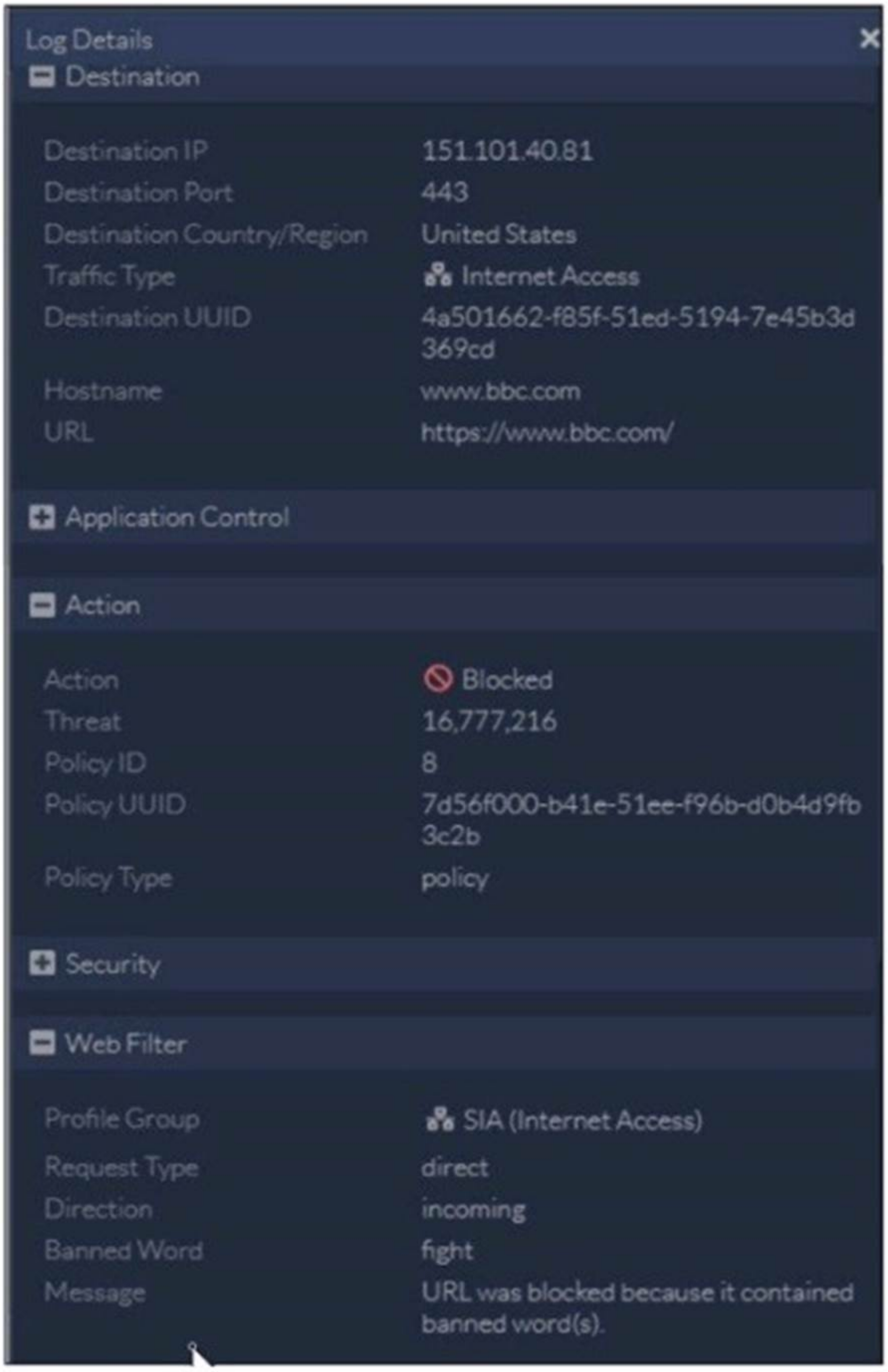
A. NAT needs to be enabled in the Spoke-to-Hub firewall policy.
B. The BGP router ID needs to match on the hub and FortiSASE.
C. FortiSASE spoke devices do not support mode config.
D. The hub needs IKEv2 enabled in the IPsec phase 1 settings.

Answer: C

Explanation:
The VPN tunnel between the FortiSASE spoke and the FortiGate hub is not establishing due to the configuration of mode config, which is not supported by FortiSASE spoke devices. Mode config is used to assign IP addresses to VPN clients dynamically, but this feature is not applicable to FortiSASE spokes.
? Mode Config in IPsec:
? Configuration Adjustment:
? Steps to Disable Mode Config:
References:
? FortiOS 7.2 Administration Guide: Provides details on configuring IPsec VPNs and mode config settings.
? FortiSASE 23.2 Documentation: Explains the supported configurations for FortiSASE spoke devices and VPN setups.

NEW QUESTION 13
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 18
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 19
.....

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