Fortinet

Exam Questions FCSS_SASE_AD-24

FCSS - FortiSASE 24 Administrator

NEW QUESTION 1
When viewing the daily summary report generated by FortiSASE. the administrator notices that the report contains very little data. What is a possible explanation for this almost empty report?

A. Digital experience monitoring is not configured.
B. Log allowed traffic is set to Security Events for all policies.
C. The web filter security profile is not set to Monitor
D. There are no security profile group applied to all policies.

Answer: B

Explanation:
If the daily summary report generated by FortiSASE contains very little data, one possible explanation is that the "Log allowed traffic" setting is configured to log only "Security Events" for all policies. This configuration limits the amount of data logged, as it only includes security events and excludes normal allowed traffic.
? Log Allowed Traffic Setting:
? Impact on Report Data:
References:
? FortiOS 7.2 Administration Guide: Provides details on configuring logging settings for traffic policies.
? FortiSASE 23.2 Documentation: Explains the impact of logging configurations on report generation and data visibility.

NEW QUESTION 2
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.)

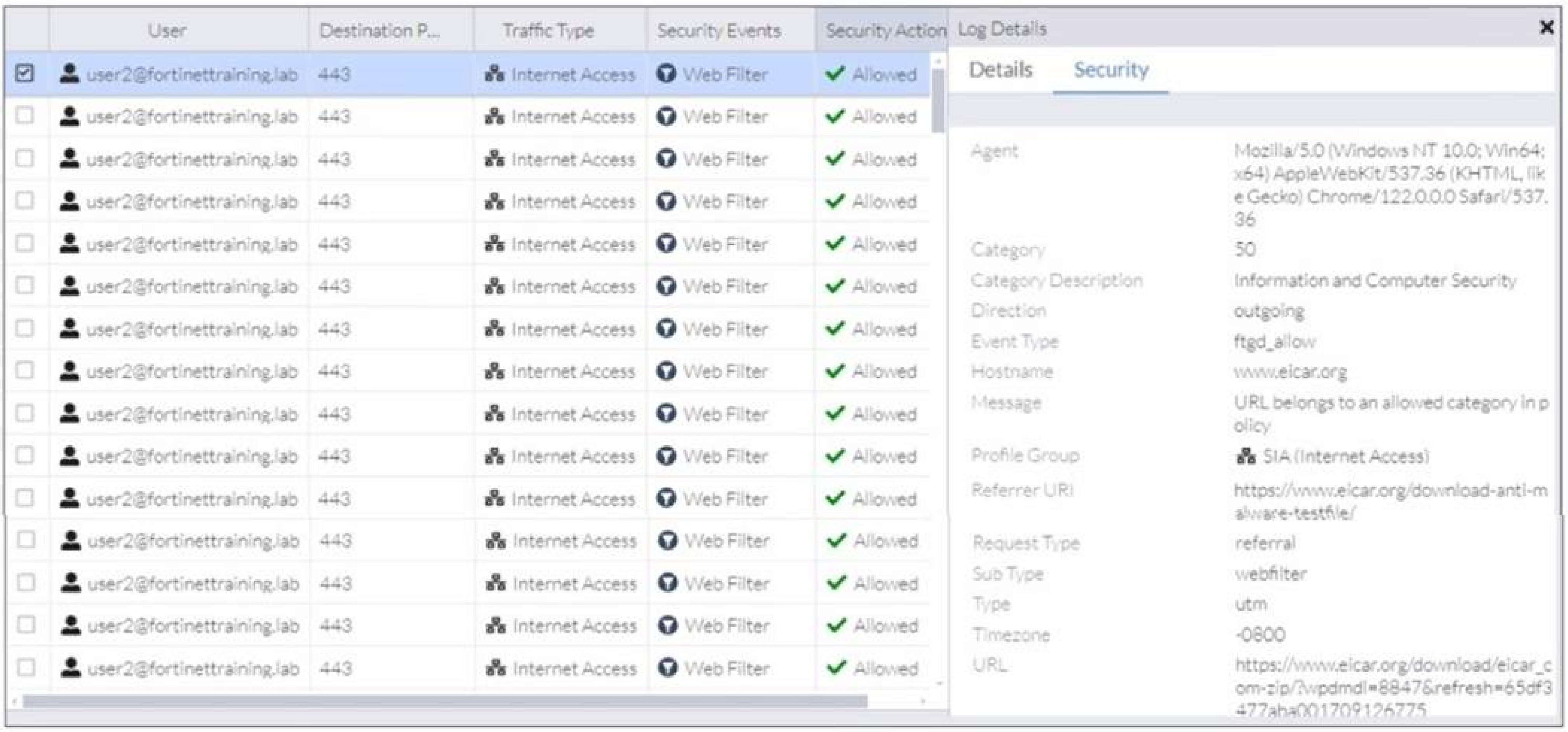
A. Add the FortiGate IP address in the secure private access configuration on FortiSASE.
B. Use the FortiClient EMS cloud connector on the corporate FortiGate to connect to FortiSASE
C. Register FortiGate and FortiSASE under the same FortiCloud account.
D. Authorize the corporate FortiGate on FortiSASE as a ZTNA access proxy.
E. Apply the FortiSASE zero trust network access (ZTNA) license on the corporate FortiGate.

Answer: BCD

Explanation:
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 3
Refer to the exhibits.

Web Filtering logs



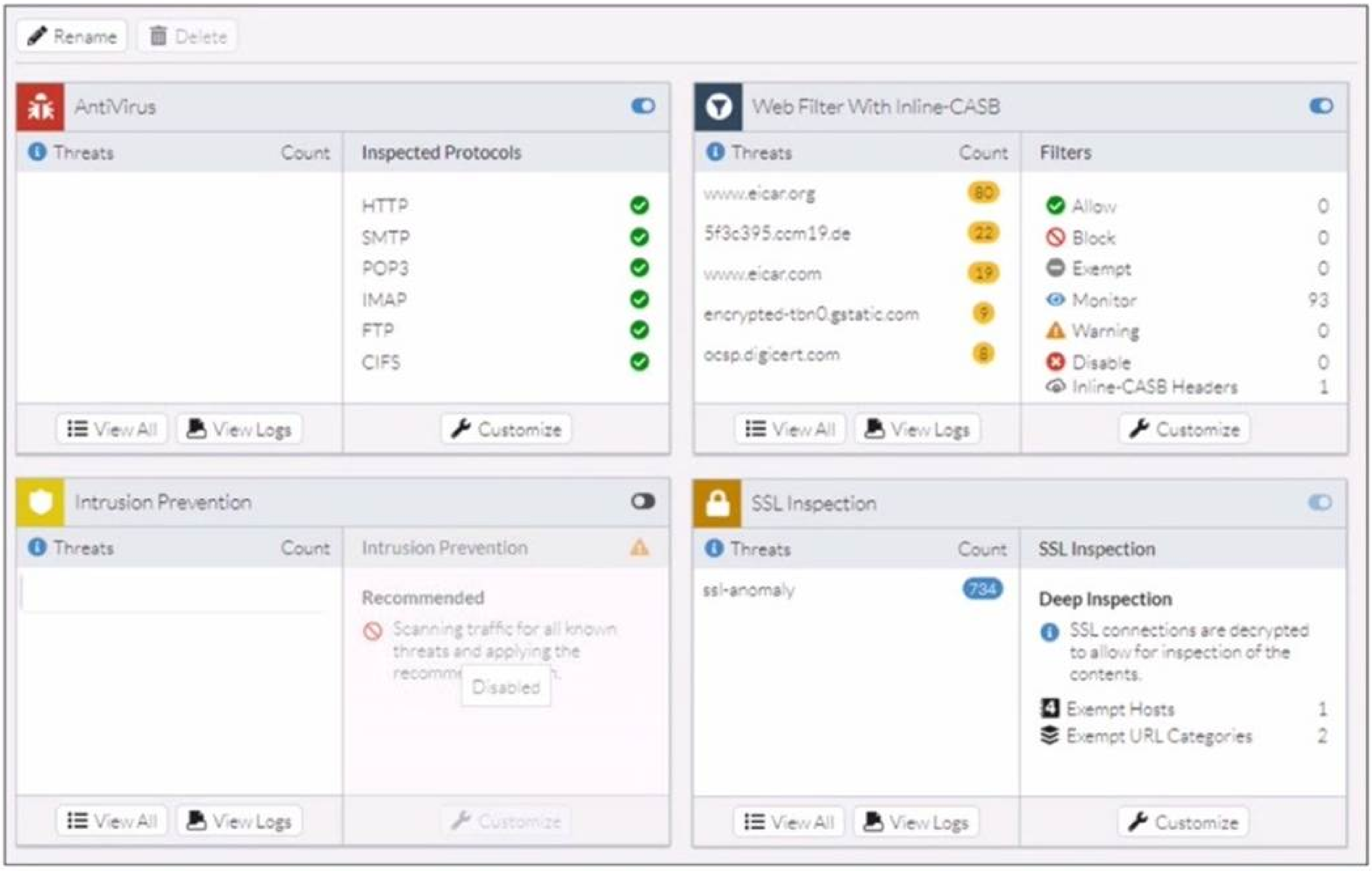
	User	Destination P...	Traffic Type	Security Events	Security Action
☑	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed
□	user2@fortinettraining.lab	443	Internet Access	Web Filter	✓ Allowed

Log Details ✕

Details Security

Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Category	50
Category Description	Information and Computer Security
Direction	outgoing
Event Type	ftgd_allow
Hostname	www.eicar.org
Message	URL belongs to an allowed category in policy
Profile Group	SIA (Internet Access)
Referrer URI	https://www.eicar.org/download-anti-malware-testfile/
Request Type	referral
Sub Type	webfilter
Type	utm
Timezone	-0800
URL	https://www.eicar.org/download/eicar_com-zip/?wpdmdl=8847&refresh=65df3477aba001709126775

Security Profile Group



AntiVirus

Threats	Count

Inspected Protocols	
HTTP	✓
SMTP	✓
POP3	✓
IMAP	✓
FTP	✓
CIFS	✓

Web Filter With Inline-CASB

Threats	Count
www.eicar.org	80
5f3c395.ccm19.de	22
www.eicar.com	19
encrypted-tbn0.gstatic.com	9
ocsp.digicert.com	8

Filters	
Allow	0
Block	0
Exempt	0
Monitor	93
Warning	0
Disable	0
Inline-CASB Headers	1

Intrusion Prevention

Threats	Count

Intrusion Prevention

Recommended

Scanning traffic for all known threats and applying the recomm Disabled n.

SSL Inspection

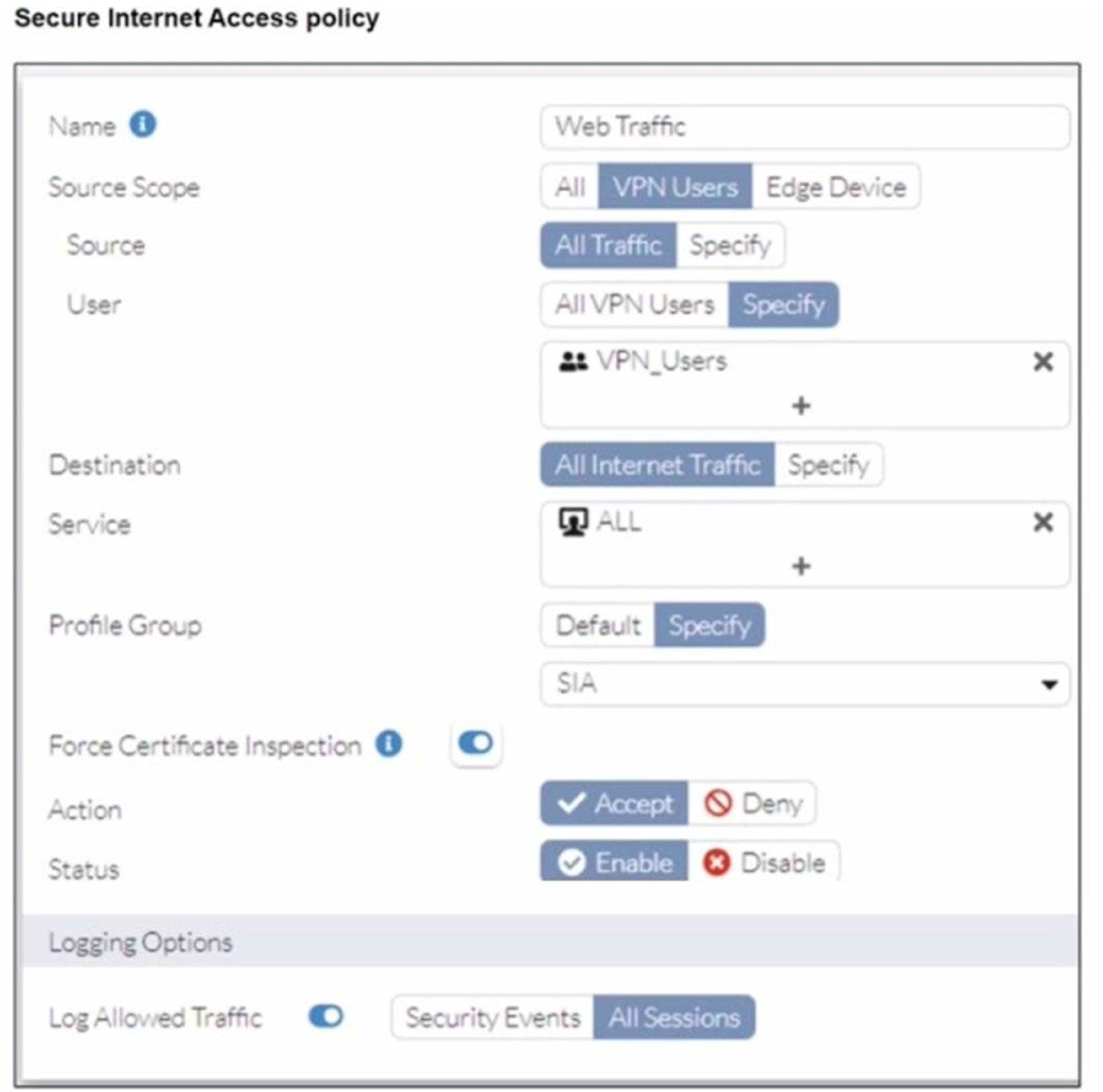
Threats	Count
ssl-anomaly	734

SSL Inspection

Deep Inspection

SSL connections are decrypted to allow for inspection of the contents.

Exempt Hosts	1
Exempt URL Categories	2



Secure Internet Access policy

Name: Web Traffic

Source Scope: All [✓ VPN Users] Edge Device

Source: [✓ All Traffic] Specify

User: All VPN Users [✓ Specify]

VPN_Users

Destination: [✓ All Internet Traffic] Specify

Service: ALL

Profile Group: Default [✓ Specify]

SIA

Force Certificate Inspection: ●

Action: [✓ Accept] Deny

Status: [✓ Enable] Disable

Logging Options

Log Allowed Traffic: ● Security Events [✓ All Sessions]

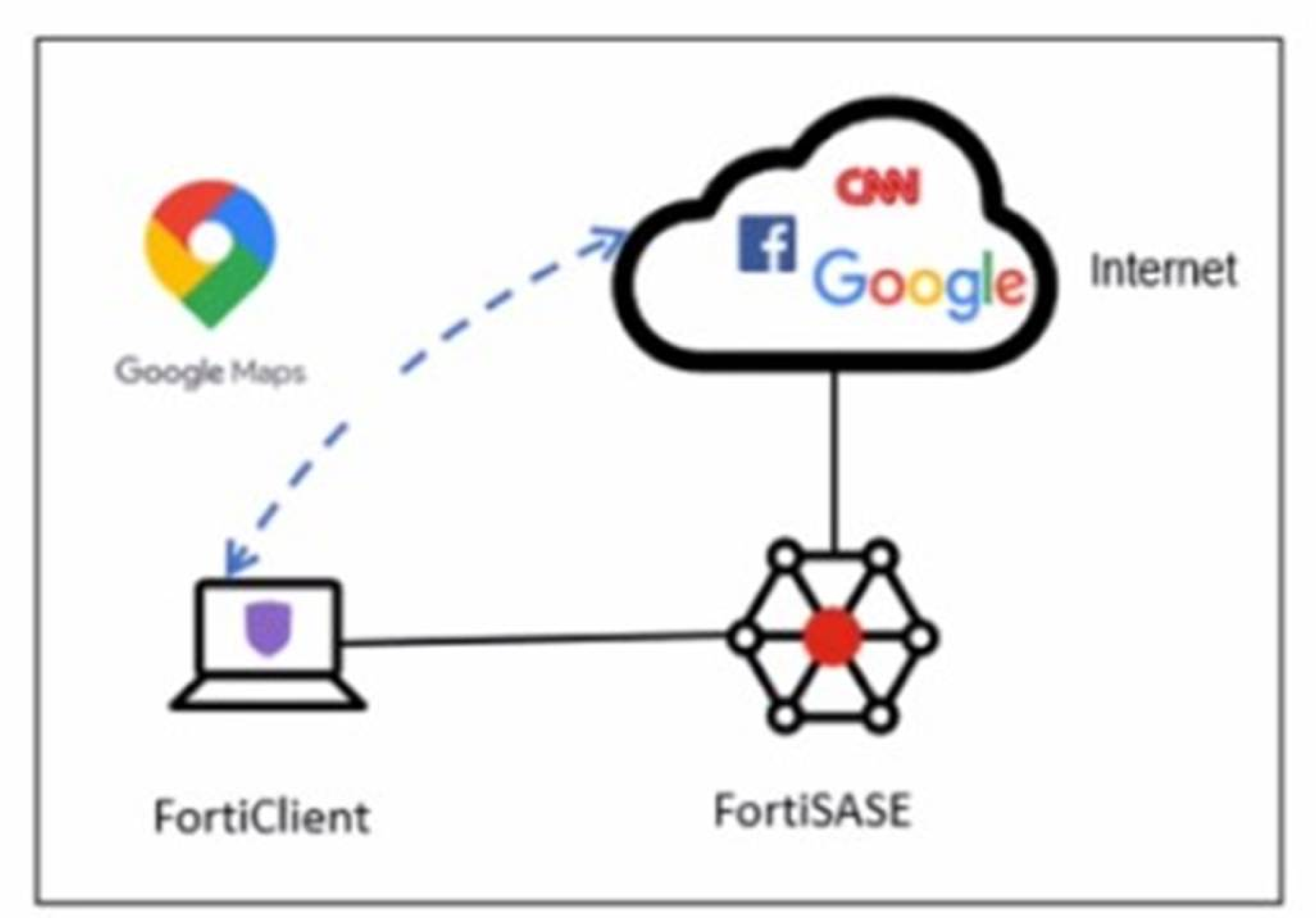
A FortiSASE administrator has configured an antivirus profile in the security profile group and applied it to the internet access policy. Remote users are still able to download the eicar.com-zip file from https://eicar.org. Traffic logs show traffic is allowed by the policy.
Which configuration on FortiSASE 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 4
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 5
A customer needs to implement device posture checks for their remote endpoints while accessing the protected server. They also want the TCP traffic between the remote endpoints and the protected servers to be processed by FortiGate.
In this scenario, which three setups will achieve the above requirements? (Choose three.)

A. Configure ZTNA tags on FortiGate.
B. Configure FortiGate as a zero trust network access (ZTNA) access proxy.
C. Configure ZTNA servers and ZTNA policies on FortiGate.
D. Configure private access policies on FortiSASE with ZTNA.
E. Sync ZTNA tags from FortiSASE to FortiGate.

Answer: ABC

Explanation:
To meet the requirements of implementingdevice posture checksfor remote endpoints and ensuringthatTCP trafficbetween the endpoints and protected servers is processed by FortiGate, the following three setups are necessary:
? Configure ZTNA tags on FortiGate (Option A):ZTNA (Zero Trust Network Access) tags are used to define access control policies based on the security posture of devices. By configuring ZTNA tags on FortiGate, administrators can enforce granular access controls, ensuring that only compliant devices can access protected resources.
? Configure FortiGate as a zero trust network access (ZTNA) access proxy (Option B):FortiGate can act as a ZTNA access proxy, which allows it to mediate and

secure connections between remote endpoints and protected servers. This setup ensures that all TCP traffic passes through FortiGate, enabling inspection and enforcement of security policies.
? Configure ZTNA servers and ZTNA policies on FortiGate (Option C):To enable ZTNA functionality, administrators must define ZTNA servers (the protected resources) and create ZTNA policies on FortiGate. These policies determine how traffic is routed, inspected, and controlled based on device posture and user identity.
Here??s why the other options are incorrect:
? D. Configure private access policies on FortiSASE with ZTNA:While FortiSASE supports ZTNA, the requirement specifies that TCP traffic must be processed by FortiGate. Configuring private access policies on FortiSASE would route traffic through FortiSASE instead of FortiGate, which does not meet the stated requirements.
? E. Sync ZTNA tags from FortiSASE to FortiGate:Synchronizing ZTNA tags is unnecessary in this scenario because the focus is on FortiGate processing the traffic. The tags can be directly configured on FortiGate without involving FortiSASE.
References:
? Fortinet FCSS FortiSASE Documentation - Zero Trust Network Access (ZTNA) Deployment
? FortiGate Administration Guide - ZTNA Configuration
================

NEW QUESTION 6
Your organization is currently using FortiSASE for its cybersecurity. They have recently hired a contractor who will work from the HQ office and who needs temporary internet access in order to set up a web-based point of sale (POS) system.
What is the recommended way to provide internet access to the contractor?

A. Use FortiClient on the endpoint to manage internet access.
B. Use a proxy auto-configuration (PAC) file and provide secure web gateway (SWG) service as an explicit web proxy.
C. Use zero trust network access (ZTNA) and tag the client as an unmanaged endpoint.
D. Configure a VPN policy on FortiSASE to provide access to the internet.

Answer: C

Explanation:
The recommended way to provide temporary internet access to the contractor is to useZero Trust Network Access (ZTNA)and tag the client as an unmanaged endpoint. ZTNA ensures that only authorized users and devices can access specific resources, while treating all endpoints as untrusted by default. By tagging the contractor's device as an unmanaged endpoint, you can apply strict access controls and ensure that the contractor has limited access to only the necessary resources (e.g., the web-based POS system) without exposing the internal network to unnecessary risks. Here??s why the other options are less suitable:
? A. Use FortiClient on the endpoint to manage internet access:While FortiClient
provides endpoint security and management, it requires installation and configuration on the contractor's device. This may not be feasible for temporary contractors or unmanaged devices.
? B. Use a proxy auto-configuration (PAC) file and provide secure web gateway
(SWG) service as an explicit web proxy:While this approach can control web traffic, it does not provide thegranular access control and security posture validation offered by ZTNA. Additionally, managing PAC files can be cumbersome and less secure compared to ZTNA.
? D. Configure a VPN policy on FortiSASE to provide access to the internet:Using a
VPN policy would grant broader access to the network, which is not ideal for a temporary contractor. It increases the risk of unauthorized access to internal resources and does not align with the principle of least privilege.
References:
? Fortinet FCSS FortiSASE Documentation - Zero Trust Network Access (ZTNA) Use Cases
? FortiSASE Administration Guide - Managing Unmanaged Endpoints
================

NEW QUESTION 7
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 8
Which two statements describe a zero trust network access (ZTNA) private access use case? (Choose two.)

A. The security posture of the device is secure.
B. All FortiSASE user-based deployments are supported.
C. All TCP-based applications are supported.
D. Data center redundancy is offered.

Answer: AC

Explanation:
Zero Trust Network Access (ZTNA) private access use cases focus on providing secure and controlled access to private applications without exposing them to the public internet. The following two statements accurately describe ZTNA private access use cases:
? The security posture of the device is secure (Option A):ZTNA enforces strict
access controls based on the principle of least privilege. Before granting access to private applications, ZTNA evaluates the security posture of the device (e.g.,

whether it is patched, compliant, and free of malware). Only devices that meet the required security standards are granted access, ensuring that the device is secure
before allowing private access.
? All TCP-based applications are supported (Option C):ZTNA supports all TCP- based applications, enabling secure access to a wide range of private applications, including legacy systems and custom-built applications. This flexibility makes ZTNA suitable for organizations with diverse application environments.
Here??s why the other options are incorrect:
? B. All FortiSASE user-based deployments are supported:While FortiSASE supports various deployment scenarios, not all user-based deployments are automatically compatible with ZTNA. Specific configurations and requirements must be met to enable ZTNA functionality.
? D. Data center redundancy is offered:Data center redundancy is unrelated to ZTNA private access use cases. Redundancy typically pertains to infrastructure design and failover mechanisms, not access control methodologies like ZTNA.
References:
? Fortinet FCSS FortiSASE Documentation - ZTNA Private Access Overview
? FortiSASE Administration Guide - ZTNA Deployment Best Practices

NEW QUESTION 9
Which secure internet access (SIA) use case minimizes individual workstation or device setup, because you do not need to 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 10
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 10
What are two requirements to enable the MSSP feature on FortiSASE? (Choose two.)

A. Add FortiCloud premium subscription on the root FortiCloud account.
B. Configure MSSP user accounts and permissions on the FortiSASE portal.
C. Assign role-based access control (RBAC) to IAM users using FortiCloud IAM portal.
D. Enable multi-tenancy on the FortiSASE portal.

Answer: CD

Explanation:
To enable theMSSP (Managed Security Service Provider)feature on FortiSASE, two key requirements must be met:
? Assign role-based access control (RBAC) to IAM users using FortiCloud IAM
portal (Option C):RBAC is essential for managing permissions and ensuring that different customers (tenants) have appropriate access levels. The FortiCloud Identity and Access Management (IAM) portal allows administrators to define roles and assign them to users, ensuring secure and granular control over resources.
? Enable multi-tenancy on the FortiSASE portal (Option D):Multi-tenancy is a critical
feature for MSSPs, as it allows them to manage multiple customer environments (tenants) from a single FortiSASE instance. Each tenant operates independently with its own configurations, policies, and reporting, while the MSSP retains centralized control.
Here??s why the other options are incorrect:
? A. Add FortiCloud premium subscription on the root FortiCloud account:While FortiCloud subscriptions may enhance functionality, they are not specifically

required to enable the MSSP feature.
? B. Configure MSSP user accounts and permissions on the FortiSASE portal:User accounts and permissions are managed through the FortiCloud IAM portal, not directly on the FortiSASE portal.
References:
? Fortinet FCSS FortiSASE Documentation - MSSP Feature Configuration
? FortiSASE Administration Guide - Multi-Tenancy and RBAC Setup

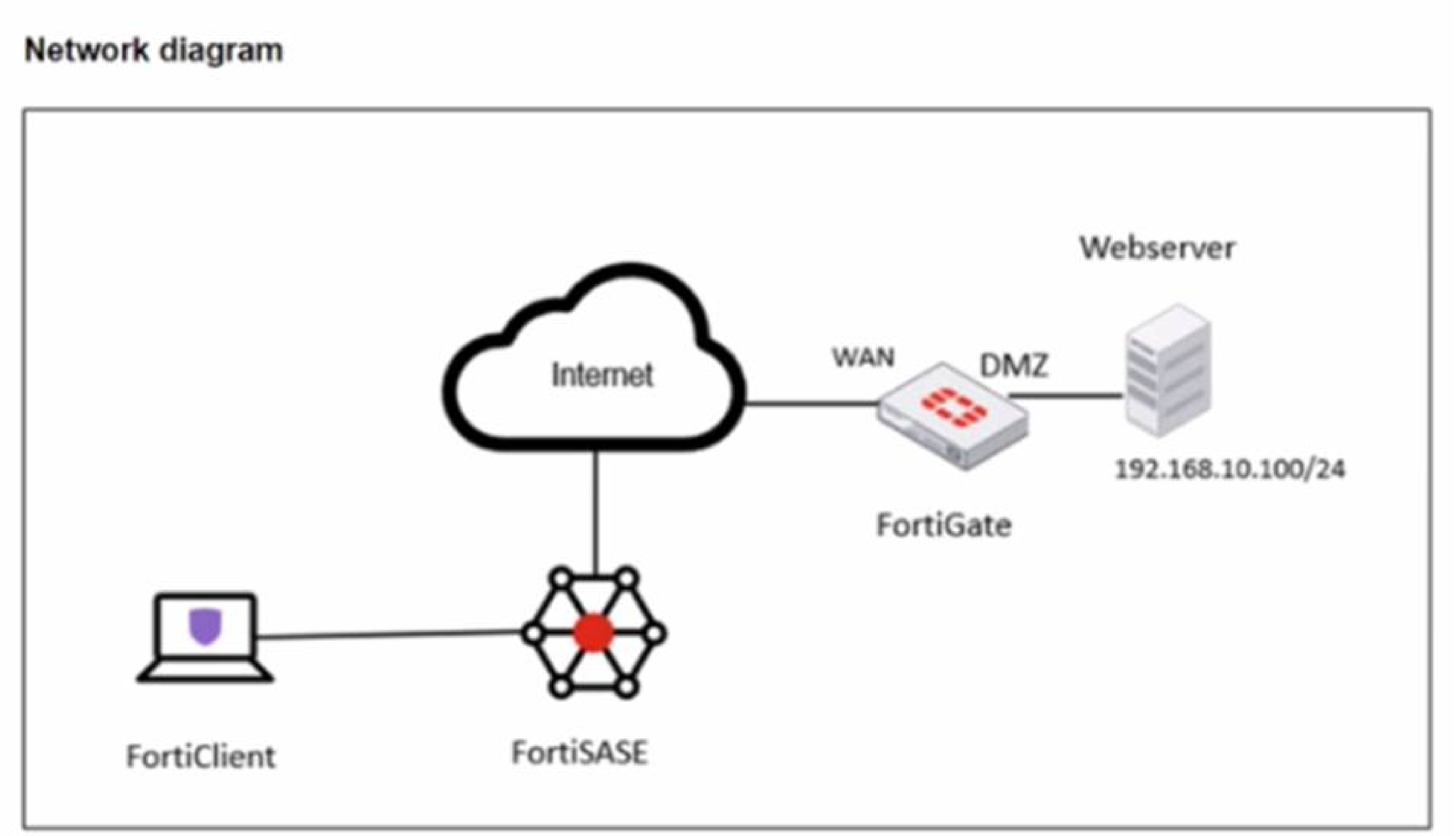
NEW QUESTION 15
Which two advantages does FortiSASE bring to businesses with multiple branch offices? (Choose two.)

A. It offers centralized management for simplified administration.
B. It enables seamless integration with third-party firewalls.
C. it offers customizable dashboard views for each branch location
D. It eliminates the need to have an on-premises firewall for each branch.

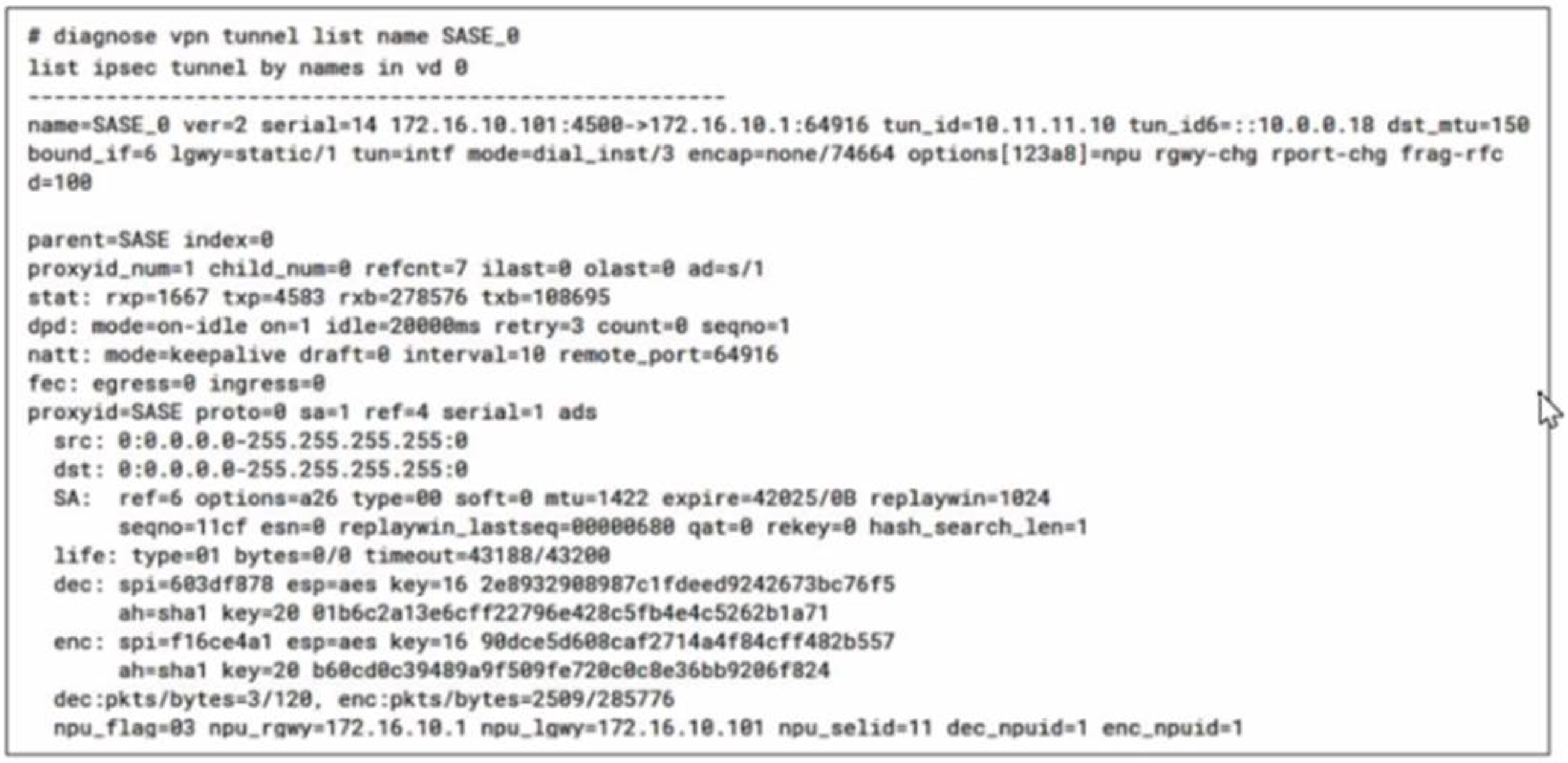
Answer: AD

Explanation:
FortiSASE brings the following advantages to businesses with multiple branch offices:
? Centralized Management for Simplified Administration:
? Eliminates the Need for On-Premises Firewalls:
References:
? FortiOS 7.2 Administration Guide: Provides information on the benefits of centralized management and cloud-based security solutions.
? FortiSASE 23.2 Documentation: Explains the advantages of using FortiSASE for businesses with multiple branch offices, including reduced need for on-premises firewalls.

NEW QUESTION 16
Refer to the exhibits.

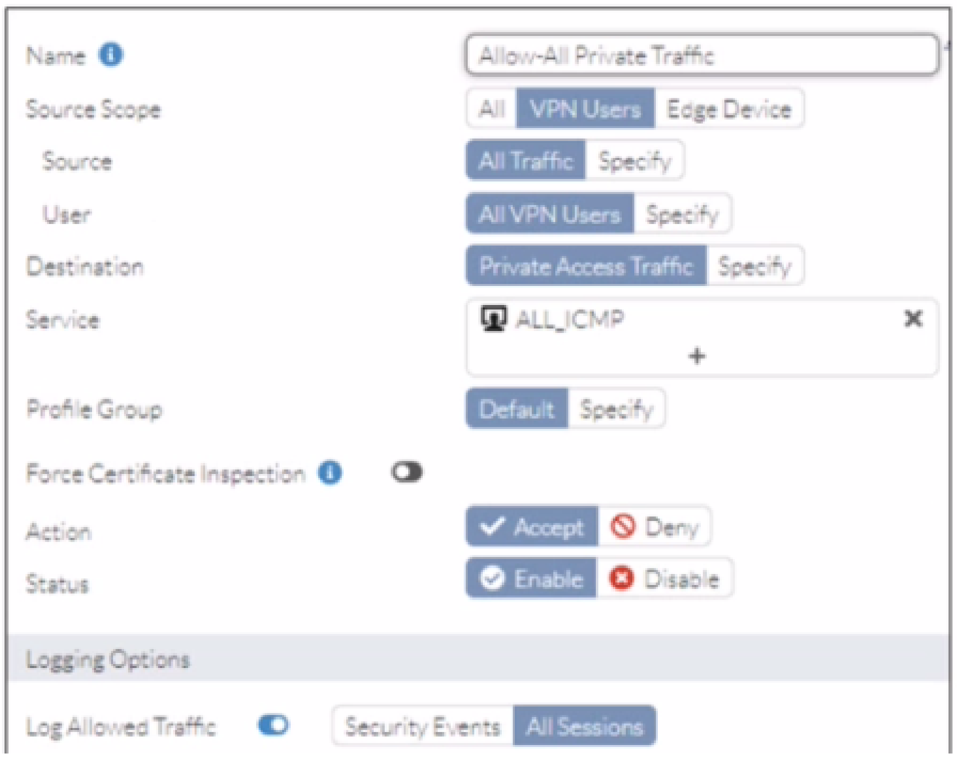


VPN tunnel diagnose output on FortiGate Hub



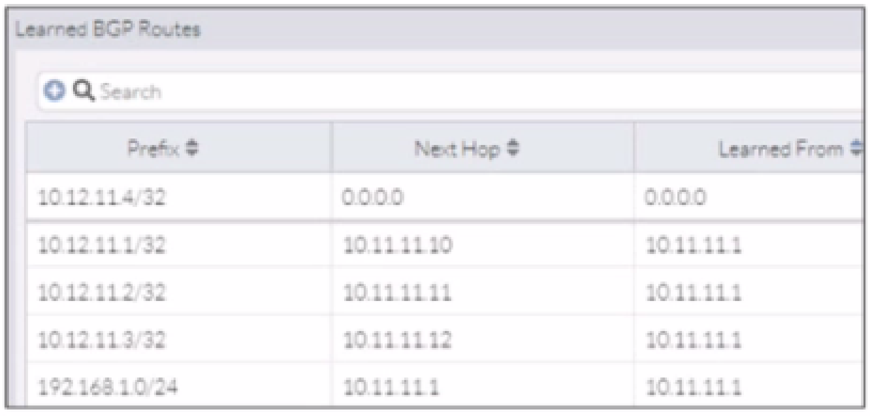
```
# diagnose vpn tunnel list name SASE_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=SASE_0 ver=2 serial=14 172.16.10.101:4500->172.16.10.1:64916 tun_id=10.11.11.10 tun_id6=::10.0.0.18 dst_mtu=150
bound_if=6 lgwy=static/1 tun=intf mode=dial_inst/3 encap=none/74664 options[123a8]=npu rgwy-chg rport-chg frag-rfc
d=100

parent=SASE index=0
proxyid_num=1 child_num=0 refcnt=7 ilast=0 olast=0 ad=s/1
stat: rxp=1667 txp=4583 rxb=278576 txb=108695
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=keepalive draft=0 interval=10 remote_port=64916
fec: egress=0 ingress=0
proxyid=SASE proto=0 sa=1 ref=4 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=6 options=a26 type=00 soft=0 mtu=1422 expire=42025/0B replaywin=1024
       seqno=11cf esn=0 replaywin_lastseq=00000680 qat=0 rekey=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=43188/43200
  dec: spi=603df878 esp=aes key=16 2e8932908987c1fdeed9242673bc76f5
       ah=sha1 key=20 01b6c2a13e6cff22796e428c5fb4e4c5262b1a71
  enc: spi=f16ce4a1 esp=aes key=16 90dce5d608caf2714a4f84cff482b557
       ah=sha1 key=20 b60cd0c39489a9f509fe720c0c8e36bb9206f824
  dec:pkts/bytes=3/120, enc:pkts/bytes=2509/285776
  npu_flag=03 npu_rgwy=172.16.10.1 npu_lgwy=172.16.10.101 npu_selid=11 dec_npuid=1 enc_npuid=1
```

Secure Private Access policy on FortiSASE



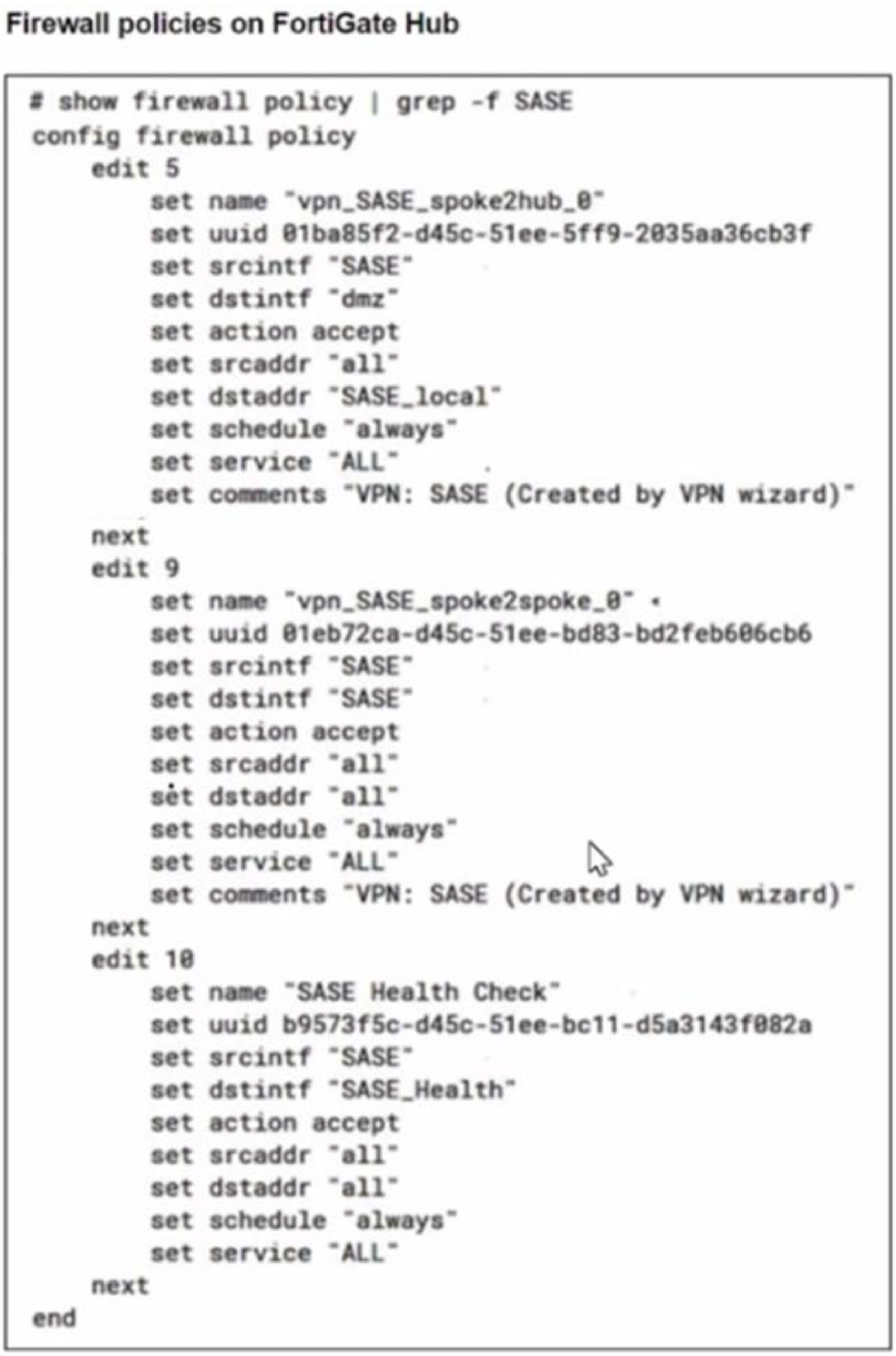
Name	Allow-All Private Traffic
Source Scope	All [✓ VPN Users] Edge Device
Source	[✓ All Traffic] Specify
User	[✓ All VPN Users] Specify
Destination	[✓ Private Access Traffic] Specify
Service	ALL_ICMP
Profile Group	[✓ Default] Specify
Force Certificate Inspection	○
Action	[✓ Accept] Deny
Status	[✓ Enable] Disable
Logging Options	
Log Allowed Traffic ●	Security Events [✓ All Sessions]

BGP route information on FortiSASE



Learned BGP Routes

Prefix	Next Hop	Learned From
10.12.11.4/32	0.0.0.0	0.0.0.0
10.12.11.1/32	10.11.11.10	10.11.11.1
10.12.11.2/32	10.11.11.11	10.11.11.1
10.12.11.3/32	10.11.11.12	10.11.11.1
192.168.1.0/24	10.11.11.1	10.11.11.1



Firewall policies on FortiGate Hub

```
# show firewall policy | grep -f SASE
config firewall policy
    edit 5
        set name "vpn_SASE_spoke2hub_0"
        set uuid 01ba85f2-d45c-51ee-5ff9-2035aa36cb3f
        set srcintf "SASE"
        set dstintf "dmz"
        set action accept
        set srcaddr "all"
        set dstaddr "SASE_local"
        set schedule "always"
        set service "ALL"
        set comments "VPN: SASE (Created by VPN wizard)"
    next
    edit 9
        set name "vpn_SASE_spoke2spoke_0"
        set uuid 01eb72ca-d45c-51ee-bd83-bd2feb606cb6
        set srcintf "SASE"
        set dstintf "SASE"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set comments "VPN: SASE (Created by VPN wizard)"
    next
    edit 10
        set name "SASE Health Check"
        set uuid b9573f5c-d45c-51ee-bc11-d5a3143f082a
        set srcintf "SASE"
        set dstintf "SASE_Health"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
    next
end
```

A FortiSASE administrator is trying to configure FortiSASE as a spoke to a FortiGate hub. The tunnel is up to the FortiGale hub. However, the administrator is not able to ping the webserver hosted behind the FortiGate hub.
Based on the output, what is the reason for the ping failures?

A. The Secure Private Access (SPA) policy needs to allow PING service.
B. Quick mode selectors are restricting the subnet.
C. The BGP route is not received.
D. Network address translation (NAT) is not enabled on the spoke-to-hub policy.

Answer: C

NEW QUESTION 19
In which three ways does FortiSASE help organizations ensure secure access for remote workers? (Choose three.)

A. It enforces multi-factor authentication (MFA) to validate remote users.
B. It secures traffic from endpoints to cloud applications.
C. It uses the identity & access management (IAM) portal to validate the identities of remote workers.
D. It offers zero trust network access (ZTNA) capabilities.
E. It enforces granular access policies based on user identities.

Answer: BDE

Explanation:

FortiSASE provides several features to ensure secure access for remote workers. The following three ways are particularly relevant:
? It secures traffic from endpoints to cloud applications (Option B):FortiSASE
secures all traffic between remote endpoints and cloud applications by inspecting it in real time. This includes applying security policies, threat detection, and data protection measures to ensure that traffic is safe and compliant.
? It offers zero trust network access (ZTNA) capabilities (Option D):ZTNA ensures
that remote workers are granted access to resources based on strict verification of their identity and device posture. By treating all users and devices as untrusted by default, ZTNA minimizes the risk of unauthorized access and lateral movement within the network.
? It enforces granular access policies based on user identities (Option E):FortiSASE
allows administrators to define and enforce fine-grained access policies based on user identities, roles, and other attributes. This ensures that remote workers only have access to the resources they need, reducing the attack surface.
Here??s why the other options are incorrect:
? A. It enforces multi-factor authentication (MFA) to validate remote users:While MFA is a critical security measure, it is typically implemented through identity providers (e.g., FortiAuthenticator or third-party solutions) rather than directly through FortiSASE.
? C. It uses the identity & access management (IAM) portal to validate the identities of remote workers:FortiSASE integrates with IAM systems but does not use the IAM portal itself to validate identities. Identity validation is handled through authentication mechanisms like SAML, LDAP, or OAuth.
References:
? Fortinet FCSS FortiSASE Documentation - Secure Remote Access
? FortiSASE Administration Guide - ZTNA and Access Policies

NEW QUESTION 23
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 25
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 28
......