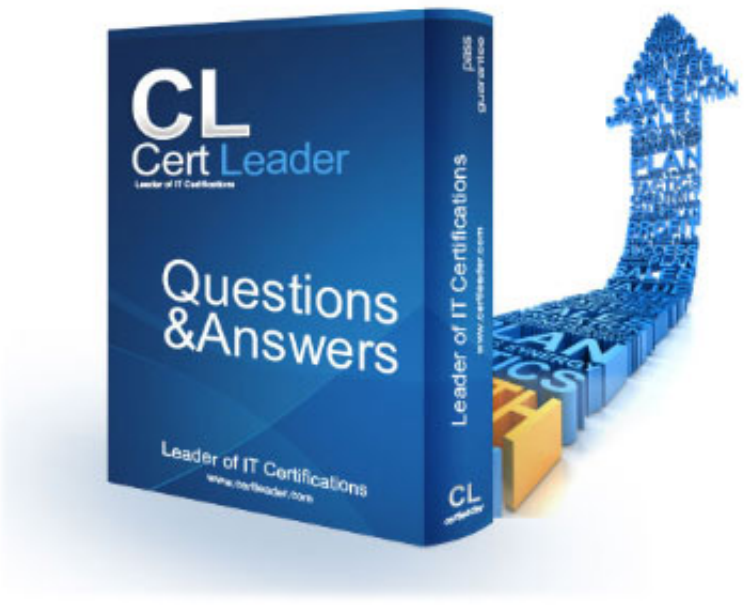
FCSS_SASE_AD-24 Dumps

FCSS - FortiSASE 24 Administrator

https://www.certleader.com/FCSS_SASE_AD-24-dumps.html



NEW QUESTION 1
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: B

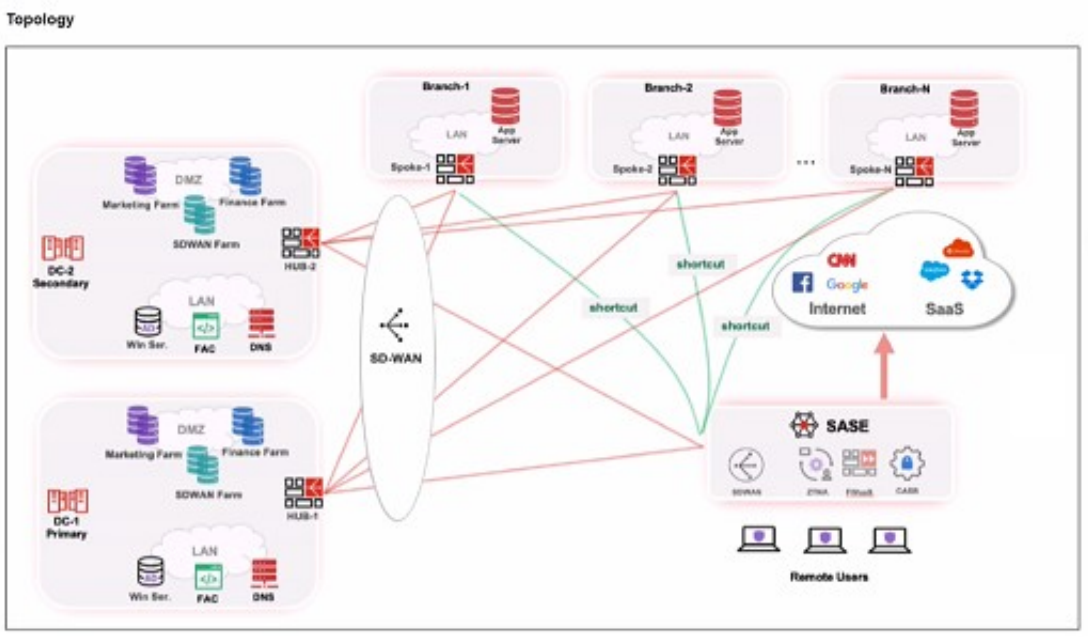
NEW QUESTION 2
A FortiSASE administrator is configuring a Secure Private Access (SPA) solution to share endpoint information with a corporate FortiGate.
Which three configuration actions will achieve this solution? (Choose three.)

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.



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: D

NEW QUESTION 4
You are designing a new network for Company X and one of the new cybersecurity policy requirements is that all remote user endpoints must always be connected and protected Which FortiSASE component facilitates this always-on security measure?

A. site-based deployment
B. thin-branch SASE extension
C. unified FortiClient
D. inline-CASB

Answer: C

Explanation:
The unified FortiClient component of FortiSASE facilitates the always-on security measure required for ensuring that all remote user endpoints are always connected and protected.
? Unified FortiClient:
? Always-On Security:
References:
? FortiOS 7.2 Administration Guide: Provides information on configuring and managing FortiClient for endpoint security.
? FortiSASE 23.2 Documentation: Explains how FortiClient integrates with
FortiSASE to deliver always-on security for remote endpoints.

NEW QUESTION 5
Refer to the exhibit.

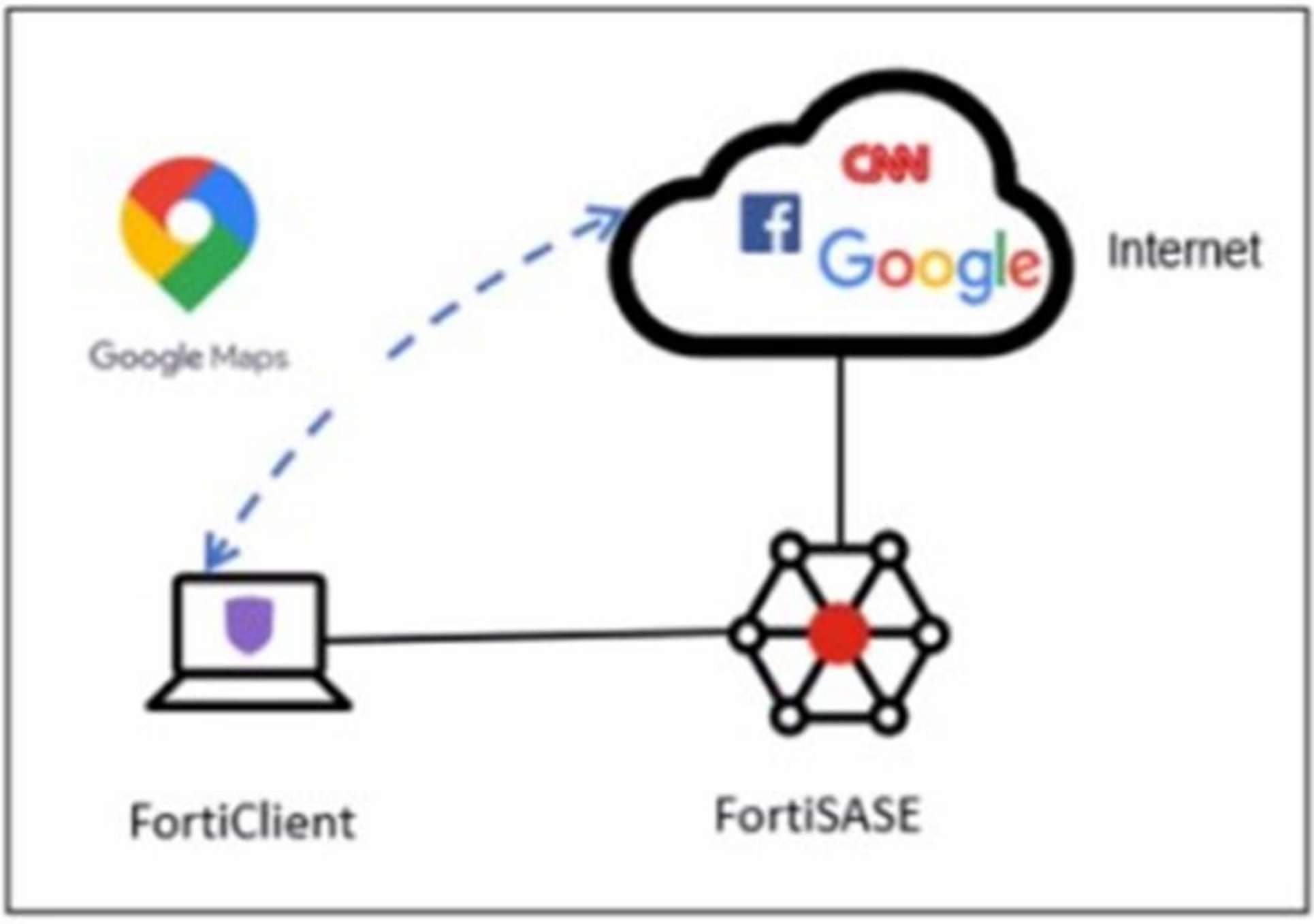
In the user connection monitor, the FortiSASE administrator notices the user name is showing random characters. Which configuration change must the administrator make to get proper user information?

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 informationin 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
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 7
Which role does FortiSASE play in supporting zero trust network access (ZTNA) principles9

A. It offers hardware-based firewalls for network segmentation.
B. It integrates with 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 8
An organization must block user attempts to log in to non-company resources while using Microsoft Office 365 to prevent users from accessing unapproved cloud resources.
Which FortiSASE feature can you implement to achieve this requirement?

A. Web Filter with Inline-CASB
B. SSL deep inspection
C. Data loss prevention (DLP)
D. Application Control with Inline-CASB

Answer: A

Explanation:
To block user attempts to log in to non-company resources while using Microsoft Office 365, theWeb Filter with Inline-CASBfeature in FortiSASE is the most appropriate solution. Inline-CASB (Cloud Access Security Broker) provides real-time visibility and control over cloud application usage. When combined with Web Filtering, it can enforce policies to restrict access to unauthorized or non-company resources within sanctioned applications like Microsoft Office 365. This ensures that users cannot access unapproved cloud resources while still allowing legitimate use of Office 365.
Here??s why the other options are incorrect:
? B. SSL deep inspection:While SSL deep inspection is useful for decrypting and inspecting encrypted traffic, it does not specifically address the need to block access to non-companyresources within Office 365. It focuses on securing traffic rather than enforcing application-specific policies.
? C. Data loss prevention (DLP):DLP is designed to prevent sensitive data from being leaked or exfiltrated. While it is a valuable security feature, it does not directly block access to non-company resources within Office 365.
? D. Application Control with Inline-CASB:Application Control focuses on managing access to specific applications rather than enforcing granular policies within an application like Office 365. Web Filter with Inline-CASB is better suited for this use case.
References:
? Fortinet FCSS FortiSASE Documentation - Inline-CASB and Web Filtering
? FortiSASE Administration Guide - Securing Cloud Applications
==========

NEW QUESTION 9
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 10
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
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.)

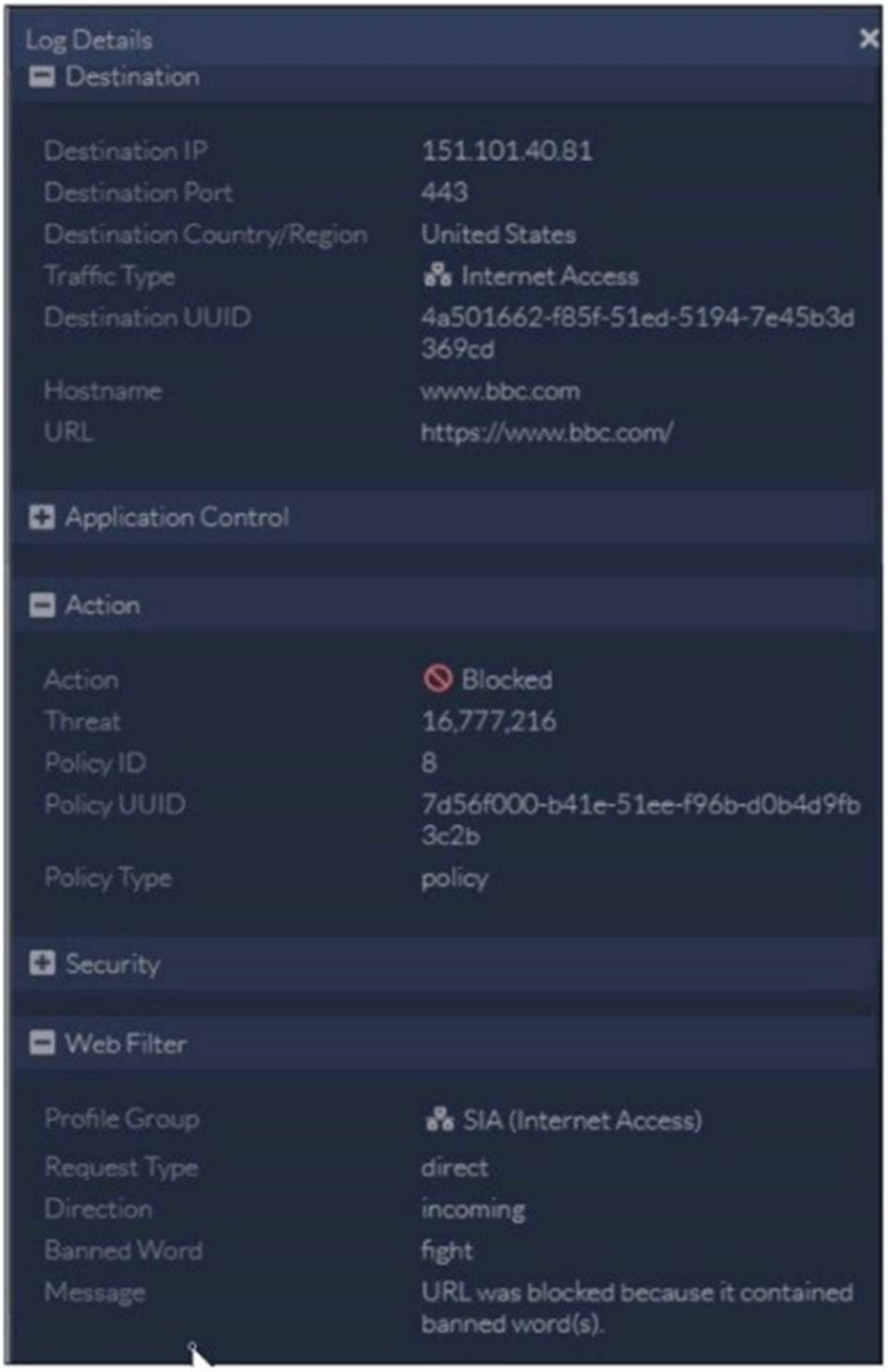
A. It offers centralized management for simplified administration.
B. It enables seamless integration with third-party firewalls.
C. it offers customizable dashboard views for each branch location
D. It eliminates the need to have an on-premises firewall for each branch.

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 19
Refer to the exhibit.

Security Logs



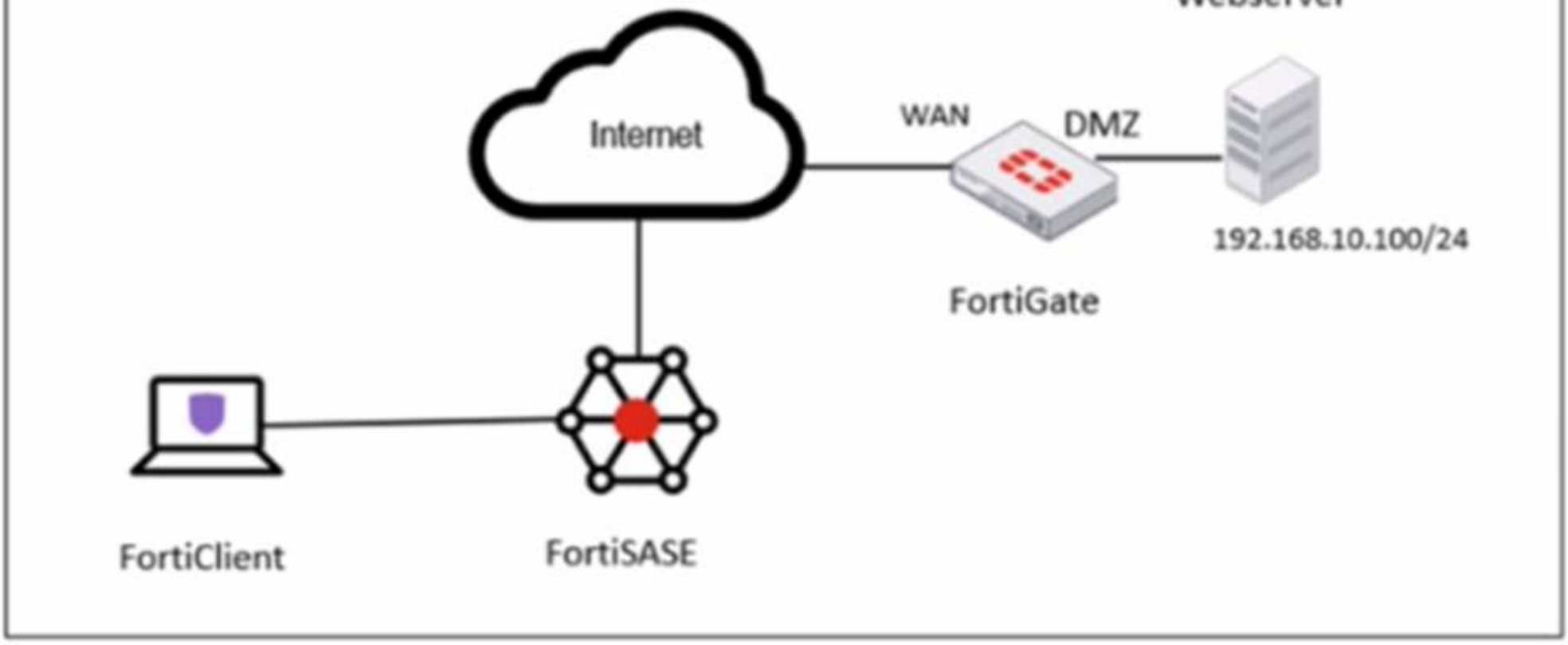
To allow access, which web tiller configuration must you change on FortiSASE?

A. FortiGuard category-based filter
B. content filter
C. URL Filter
D. inline cloud access security broker (CASB) headers

Answer: B

NEW QUESTION 22
Refer to the exhibits.

Network diagram

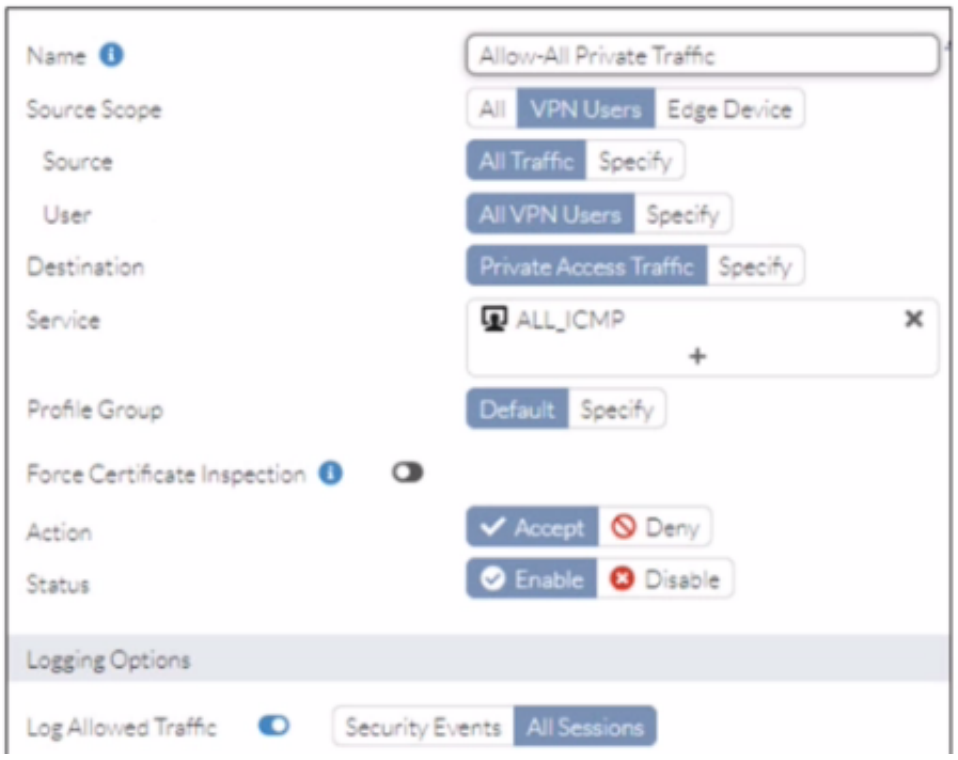


VPN tunnel diagnose output on FortiGate Hub

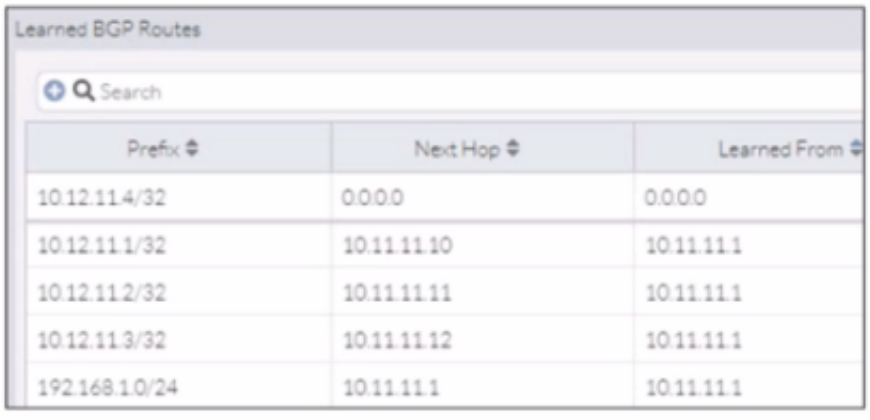
```
# diagnose vpn tunnel list name SASE_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=SASE_0 ver=2 serial=14 172.16.10.101:4500->172.16.10.1:64916 tun_id=10.11.11.10 tun_id6=::10.0.0.18 dst_mtu=150
bound_if=6 lgwy=static/1 tun=intf mode=dial_inst/3 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 2e8932988987c1fdeed9242673bc76f5
       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



BGP route information on FortiSASE



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 25
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: A

Explanation:

(https://docs.fortinet.com/document/fortisase/24.4.75/sia-agent-based-deployment- guide/568255/configuring-application-control-profile

NEW QUESTION 28
Which of the following describes the FortiSASE inline-CASB component?

A. It provides visibility for unmanaged locations and devices.
B. It is placed directly in the traffic path between the endpoint and cloud applications.
C. It uses API to connect to the cloud applications.
D. It detects data at rest.

Answer: B

Explanation:
TheFortiSASE inline-CASB (Cloud Access Security Broker)component is designed to provide real-time security and visibility by beingplaced directly in the traffic path between the endpoint and cloud applications. Inline-CASB inspects traffic as it flows to and from cloud applications, enablingenforcement of security policies, detection of threats, and prevention of unauthorized access. This approach ensures that all interactions with cloud applications are monitored and controlled in real time.
Here??s why the other options are incorrect:
? A. It provides visibility for unmanaged locations and devices:While inline-CASB enhances visibility, its primary function is to inspect and secure traffic in real time. Visibility for unmanaged locations and devices is typically achieved through other components like endpoint agents or API-based CASB.
? C. It uses API to connect to the cloud applications:API-based CASB is a different approach that relies on APIs provided by cloud applications to monitor and manage data. Inline-CASB operates directly in the traffic flow rather than using APIs.
? D. It detects data at rest:Detecting data at rest is typically handled by Data Loss Prevention (DLP) tools or API-based CASB solutions. Inline-CASB focuses on inspecting traffic in motion, not data stored in cloud applications.
References:
? Fortinet FCSS FortiSASE Documentation - Inline-CASB Overview
? FortiSASE Administration Guide - Cloud Application Security

NEW QUESTION 31
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 34
When deploying FortiSASE agent-based clients, which three features are available compared to an agentless solution? (Choose three.)

A. Vulnerability scan
B. SSL inspection
C. Anti-ransomware protection
D. Web filter
E. ZTNA tags

Answer: ACE

NEW QUESTION 36
Which statement applies to a single sign-on (SSO) deployment on FortiSASE?

A. SSO overrides any other previously configured user authentication.
B. SSO identity providers can be integrated using public and private access types.
C. SSO is recommended only for agent-based deployments.
D. SSO users can be imported into FortiSASE and added to user groups.

Answer: D

Explanation:
In aSingle Sign-On (SSO)deployment on FortiSASE,SSO users can be imported into FortiSASE and added to user groups. This allows administrators to manage SSO users within FortiSASE, enabling them to apply policies, permissions, and group-based access controls. By integrating SSO with FortiSASE, organizations can streamline user authentication and simplify access management while maintaining security. Here??s why the other options are incorrect:
? A. SSO overrides any other previously configured user authentication:This is incorrect because SSO does not automatically override other authentication methods. FortiSASE supports multiple authentication mechanisms, and SSO is just one of them. Administrators can configure fallback authentication methods if needed.
? B. SSO identity providers can be integrated using public and private access types:While FortiSASE supports integration with various identity providers (e.g., SAML, LDAP, OAuth), the concept of "public and private access types" is not applicable to SSO configurations.
? C. SSO is recommended only for agent-based deployments:This is incorrect

because SSO can be used in both agent-based and agentless deployments. It is not limited to environments where agents are installed.
References:
? Fortinet FCSS FortiSASE Documentation - Single Sign-On (SSO) Integration
? FortiSASE Administration Guide - User Authentication and SSO
==========

NEW QUESTION 40
.....

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-24 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCSS_SASE_AD-24-dumps.html