

Exam Questions FCSS_SASE_AD-24

FCSS - FortiSASE 24 Administrator

https://www.2passeasy.com/dumps/FCSS_SASE_AD-24/



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

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:

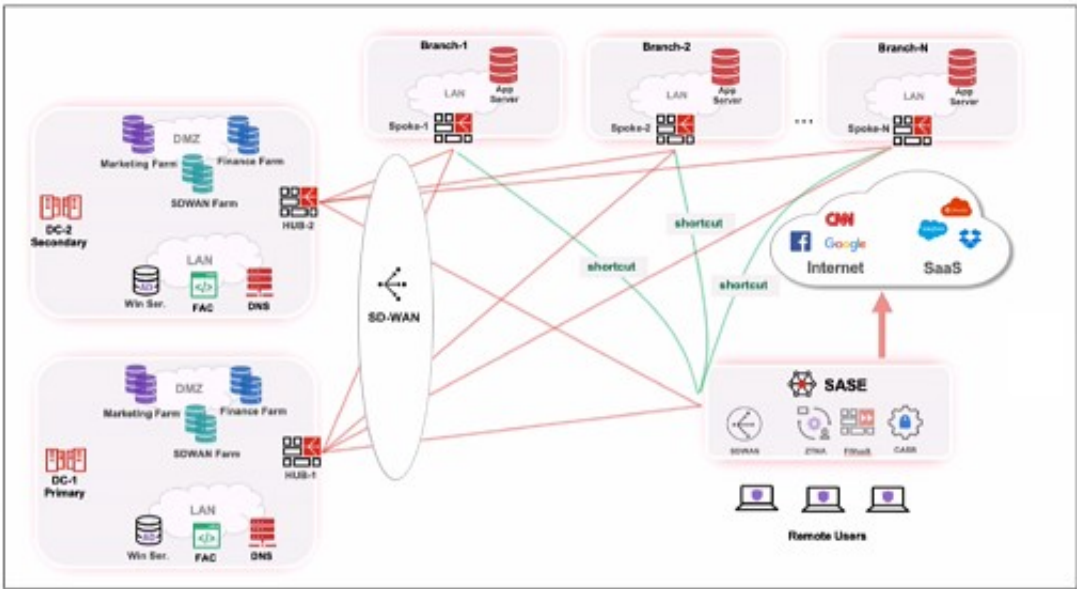
? FortiOS 7.2 Administration Guide: Provides details on configuring logging settings for traffic policies.

? FortiSASE 23.2 Documentation: Explains the impact of logging configurations on report generation and data visibility.

NEW QUESTION 3

Refer to the exhibits.

Topology



Priority settings

Set Priority ▾		Ashburn - Virginia - USA ▾	
<input type="checkbox"/>	Name	Priority ▲	
<input type="checkbox"/>	HUB-1	P1	(Highest Priority)
<input type="checkbox"/>	HUB-2	P2	

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

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

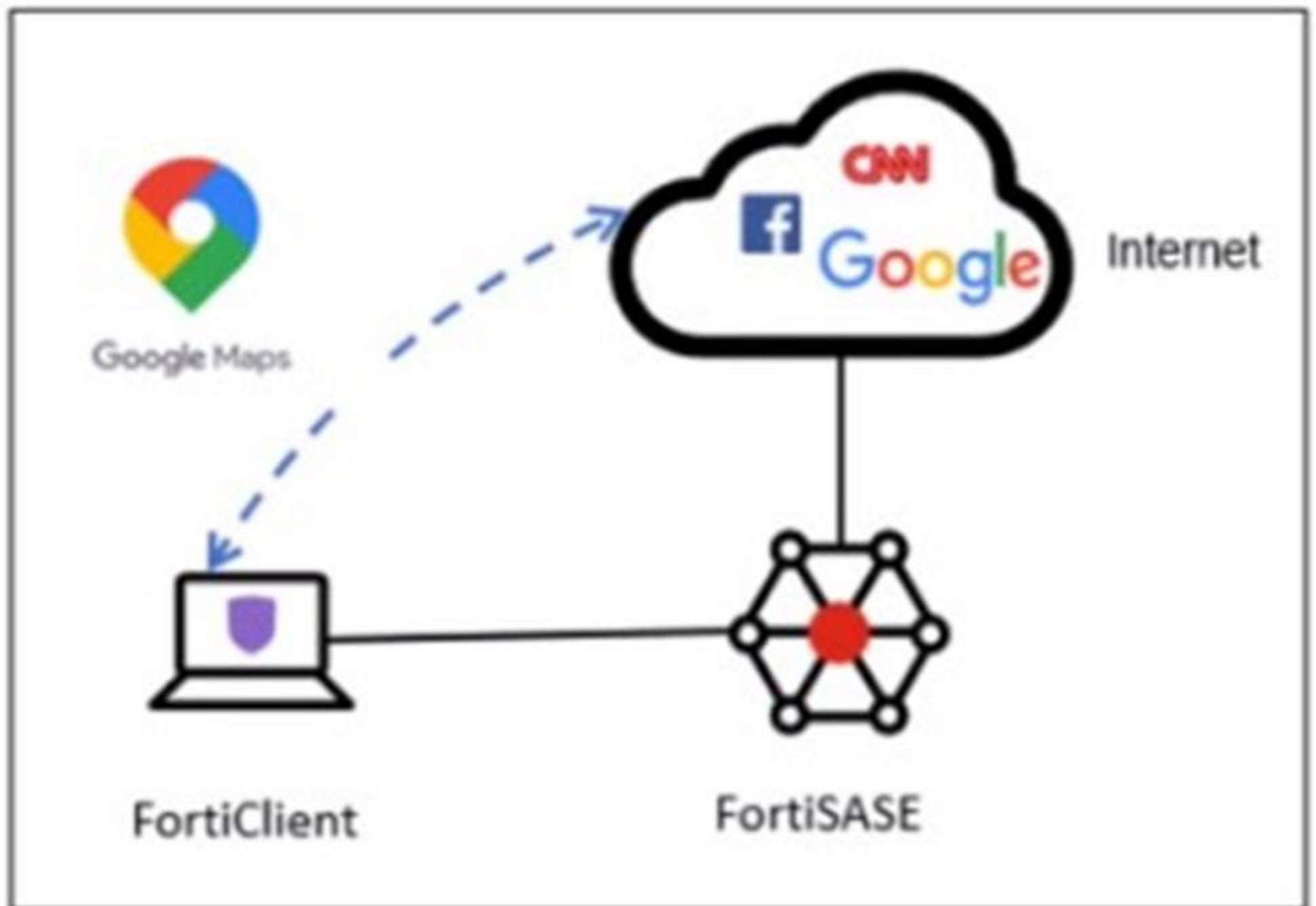
Which policy type is used to control traffic between the FortiClient endpoint to FortiSASE for secure internet access?

- A. VPN policy
- B. thin edge policy
- C. private access policy
- D. secure web gateway (SWG) policy

Answer: A

NEW QUESTION 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

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 implementing device posture checks for remote endpoints and ensuring that TCP traffic between 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 8

Which two additional components does FortiSASE use for application control to act as an inline-CASB? (Choose two.)

- A. intrusion prevention system (IPS)
- B. SSL deep inspection
- C. DNS filter
- D. Web filter with inline-CASB

Answer: AB

NEW QUESTION 9

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, the Web Filter with Inline-CASB feature 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-company resources 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 10

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 use Zero 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 the granular 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

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 14

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 endpoints?

- 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 17

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

Answer: A

Explanation:

The issue of an almost empty daily summary report in FortiSASE can often be traced back to how logging is configured within the system. Specifically, if "Log Allowed Traffic" is set to "Security Events" for all policies, it means that only security-related events (such as threats or anomalies) are being logged, while normal, allowed traffic is not being recorded. Since most traffic in a typical network environment is allowed, this configuration would result in very little data being captured and subsequently reported in the daily summary.

Here's a breakdown of why the other options are less likely to be the cause:

? B. There are no security profile groups applied to all policies: While applying security profiles is important for comprehensive protection, their absence does not directly affect the volume of data in reports unless specific logging settings are also misconfigured.

? C. The web filter security profile is not set to Monitor: This option pertains specifically to web filtering activities. Even if web filtering is not set to monitor mode, other types of traffic and logs should still populate the report.

? D. Digital experience monitoring is not configured: Digital Experience Monitoring (DEM) focuses on user experience metrics rather than general traffic logging. Its absence would not lead to an almost empty report.

To resolve this issue, administrators should review the logging settings across all policies and ensure that "Log Allowed Traffic" is appropriately configured to capture the necessary data for reporting purposes.

References:

- ? Fortinet FCSS FortiSASE Documentation - Reporting and Logging Best Practices
- ? FortiSASE Administration Guide - Configuring Logging Settings

NEW QUESTION 21

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:

The event log subtype that 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.

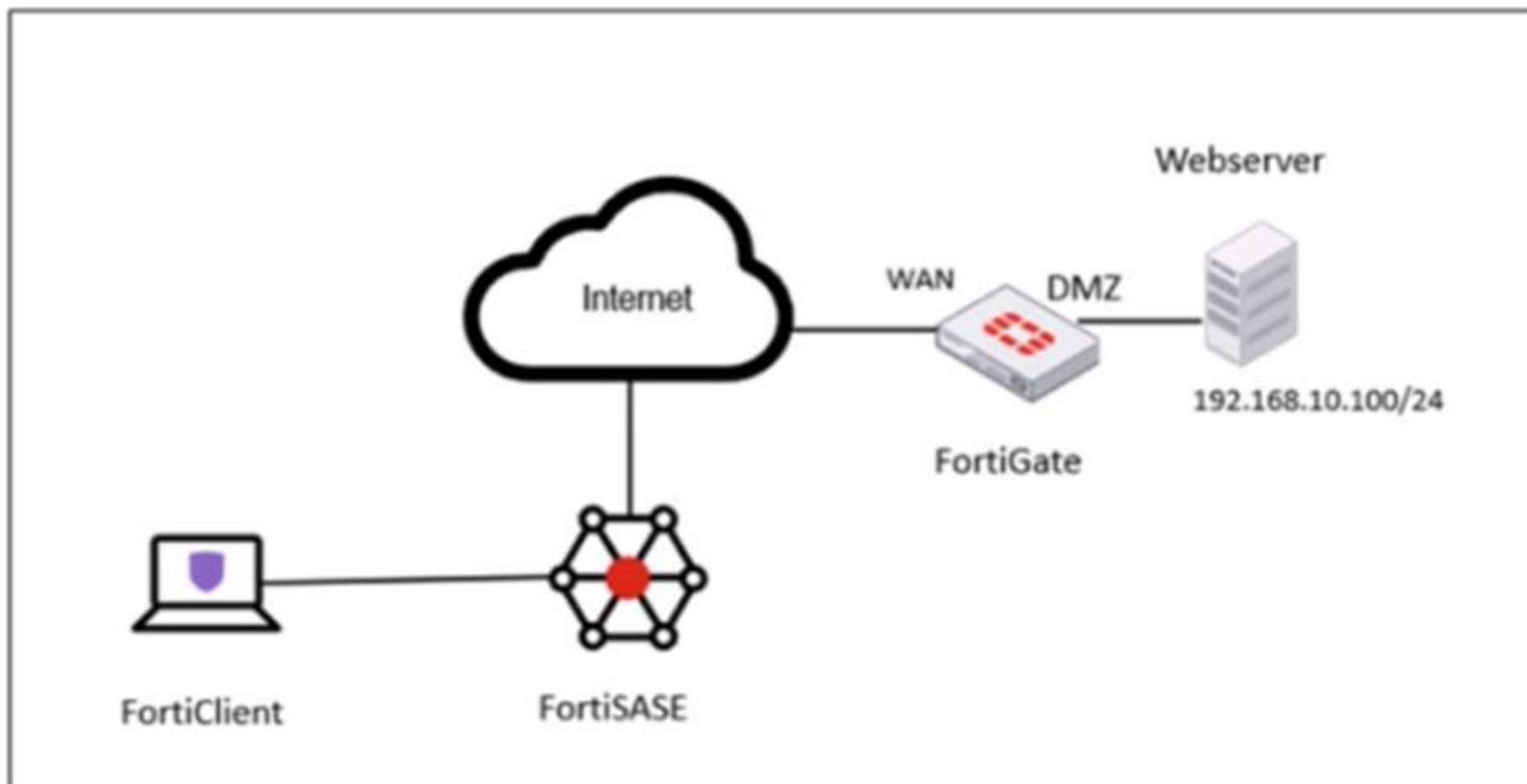
References:

- ? Fortinet FCSS FortiSASE Documentation - Event Logging and Subtypes
- ? FortiSASE Administration Guide - Monitoring and Logging

NEW QUESTION 26

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=ntf 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=42025/00 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

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		
🔍 Search		
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 FortiGate 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 31

Refer to the exhibits.

Managed Endpoints

Endpoint	VPN Username	Management Connection	ZTNA Tags (Simple)	FortiClient Version	Vulnerabilities Detected
Win10-Pro	use2@fortinettraininglab	Online	FortiSASE-Compliant	7.0.10.0538	140
Win7-Pro	use1@fortinettraininglab	Online	FortiSASE-Non-Compliant, FortiSASE-Compliant	7.0.8.0427	176

Secure Internet Access Policy

<div> <div>+ Create</div> <div>Edit</div> <div>Delete</div> <div>Search</div> </div>						
<input type="checkbox"/>	Name	Profile Group	Source	User	Destination	Action
<input type="checkbox"/>	Botnet Deny		all	All VPN Users	Botnet-C&C Server	Deny
<input type="checkbox"/>	Non-Compliant		FortiSASE-Non-Compliant	All VPN Users	All Internet Traffic	Deny
<input type="checkbox"/>	Web Traffic	SIA	FortiSASE-Compliant	VPN_Users	All Internet Traffic	Accept
<input type="checkbox"/>	Allow-All	Default		All VPN Users	All Internet Traffic	Accept
<input type="checkbox"/>	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 through 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 34

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 38

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 42

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:

The FortiSASE inline-CASB (Cloud Access Security Broker) component is designed to provide real-time security and visibility by being placed directly in the traffic path between the endpoint and cloud applications. Inline-CASB inspects traffic as it flows to and from cloud applications, enabling enforcement 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 43

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:

The Digital Experience Monitor (DEM) feature in FortiSASE is designed to provide end-to-end network visibility by 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 47

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_SASE_AD-24 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_SASE_AD-24 Product From:

https://www.2passeasy.com/dumps/FCSS_SASE_AD-24/

Money Back Guarantee

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