

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

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

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 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.



Security Profile Group

Rename Delete

Antivirus

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

View All View Logs Customize

Web Filter With Inline-CASB

Threats	Count	Filters
www.eicar.org	80	Allow 0
5f3c395.com19.de	22	Block 0
www.eicar.com	19	Exempt 0
encrypted-tbn0.gstatic.com	9	Monitor 93
ocsp.digicert.com	8	Warning 0
		Disable 0
		Inline-CASB Headers 1

View All View Logs Customize

Intrusion Prevention

Threats	Count	Intrusion Prevention
		<div>Recommended</div> <div>Scanning traffic for all known threats and applying the recommended settings.</div> <div>Disabled</div>

View All View Logs Customize

SSL Inspection

Threats	Count	SSL Inspection
ssl-anomaly	734	<div>Deep Inspection</div> <div>SSL connections are decrypted to allow for inspection of the contents.</div> <div>4 Exempt Hosts 1</div> <div>Exempt URL Categories 2</div>

View All View Logs Customize

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 X
	+
Destination	All Internet Traffic Specify
Service	ALL X
	+
Profile Group	Default Specify
	SIA
Force Certificate Inspection	<input checked="" type="checkbox"/>
Action	Accept Deny
Status	Enable Disable
Logging Options	
Log Allowed Traffic	<input checked="" type="checkbox"/>
	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 7

Which secure internet access (SIA) use case minimizes individual endpoint configuration?

- A. Site-based remote user internet access
- B. Agentless remote user internet access
- C. SIA for SSL VPN remote users
- D. SIA using ZTNA

Answer: B

Explanation:

The agentless remote user internet access use case is designed to minimize individual endpoint configuration. In this scenario, FortiSASE provides secure internet access without requiring the installation of an agent on the endpoint device. This approach is particularly useful for environments with unmanaged devices or temporary users, as it eliminates the need for complex configurations on each endpoint. Instead, security policies are enforced at the network level, ensuring consistent protection without relying on endpoint-specific software.

Here's why the other options are incorrect:

? A. Site-based remote user internet access: This use case involves securing internet access for users at a specific site or location, typically through a gateway or firewall. While it simplifies configuration for all users at that site, it does not specifically minimize individual endpoint configuration for remote users.

? C. SIA for SSL VPN remote users: SSL VPN requires users to connect to the corporate network via a client or browser-based interface. This approach often involves additional configuration on the endpoint, such as installing and configuring the SSL VPN client.

? D. SIA using ZTNA: Zero Trust Network Access (ZTNA) focuses on verifying the identity and posture of devices before granting access to resources. While ZTNA enhances security, it may require endpoint agents or posture checks, which involve some level of endpoint configuration.

References:

? Fortinet FCSS FortiSASE Documentation - Secure Internet Access (SIA) Use Cases

? FortiSASE Administration Guide - Agentless Remote User Access

NEW QUESTION 8

How does FortiSASE hide user information when viewing and analyzing logs?

- A. By hashing data using Blowfish
- B. By hashing data using salt
- C. By encrypting data using Secure Hash Algorithm 256-bit (SHA-256)
- D. By encrypting data using advanced encryption standard (AES)

Answer: B

Explanation:

FortiSASE hides user information when viewing and analyzing logs by hashing data using salt. This approach ensures that sensitive user information is obfuscated, enhancing privacy and security.

? Hashing Data with Salt:

? Security and Privacy:

References:

? FortiOS 7.2 Administration Guide: Provides information on log management and data protection techniques.

? FortiSASE 23.2 Documentation: Details on how FortiSASE implements data hashing and salting to secure user information in logs.

NEW QUESTION 9

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 10

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 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 14

Which statement describes the FortiGuard forensics analysis feature on FortiSASE?

- A. It can help troubleshoot user-to-application performance issues.
- B. It can help customers identify and mitigate potential risks to their network.
- C. It can monitor endpoint resources in real-time.
- D. It is a 24x7x365 monitoring service of your FortiSASE environment.

Answer: B

Explanation:

The FortiGuard forensics analysis feature on FortiSASE is designed to help customers identify and mitigate potential risks to their network. This feature provides detailed insights into suspicious activities, threats, and anomalies detected by FortiSASE. By analyzing logs, traffic patterns, and threat intelligence, FortiGuard forensics enables administrators to investigate incidents, understand their root causes, and take proactive measures to secure the network.

Here's why the other options are incorrect:

? A. It can help troubleshoot user-to-application performance issues: Performance troubleshooting is typically handled by features like Digital Experience Monitoring (DEM) or application performance monitoring tools, not forensics analysis.

? C. It can monitor endpoint resources in real-time: Real-time endpoint monitoring is a function of endpoint security solutions like FortiClient or FortiEDR, not FortiGuard forensics analysis.

? D. It is a 24x7x365 monitoring service of your FortiSASE environment: While Fortinet offers managed services for continuous monitoring, FortiGuard forensics analysis is not a dedicated monitoring service. Instead, it focuses on post-incident investigation and risk mitigation.

References:

? Fortinet FCSS FortiSASE Documentation - FortiGuard Forensics Analysis

? FortiSASE Administration Guide - Threat Detection and Response

NEW QUESTION 17

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 the MSSP (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:

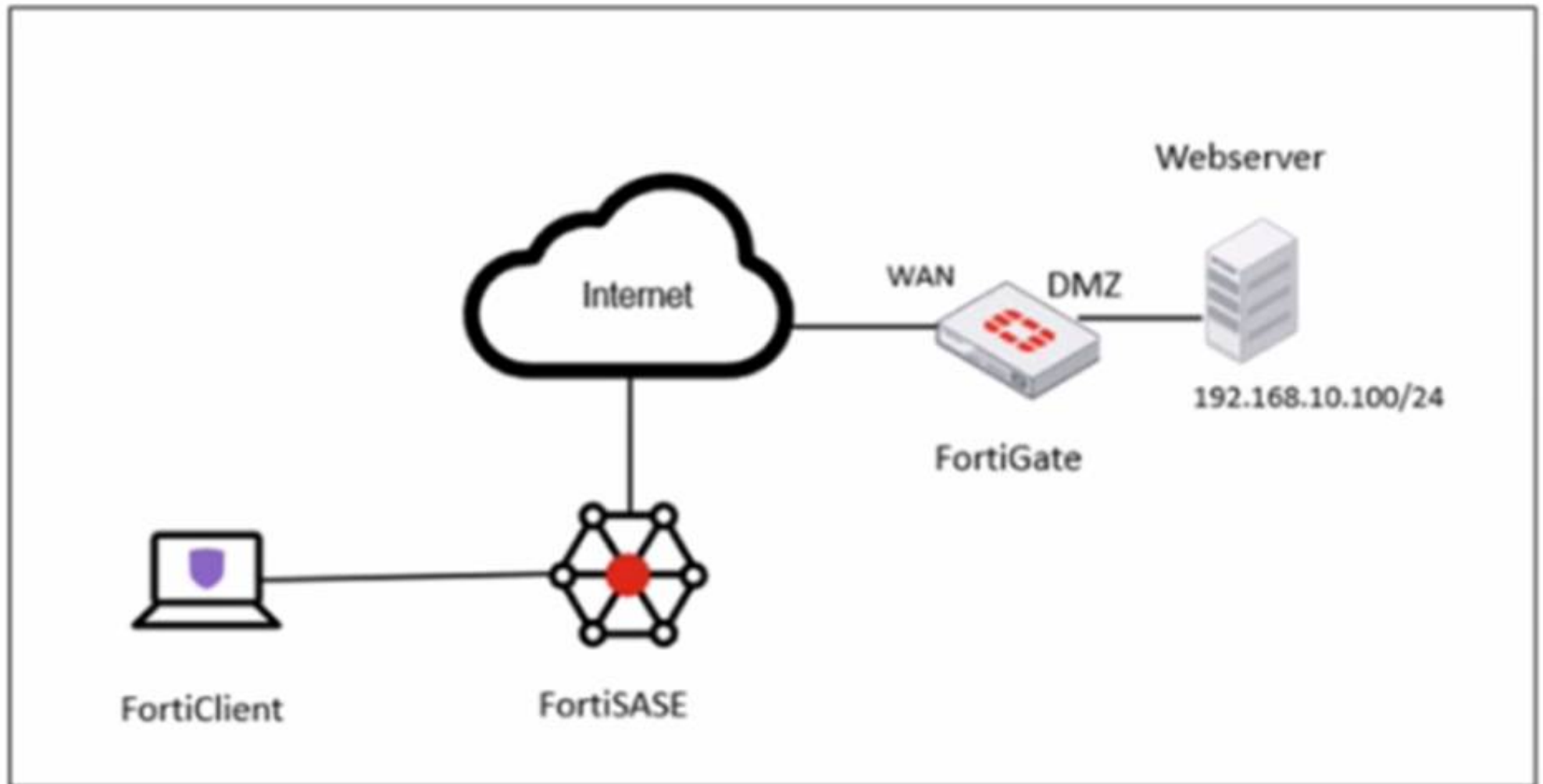
? Fortinet FCSS FortiSASE Documentation - MSSP Feature Configuration

? FortiSASE Administration Guide - Multi-Tenancy and RBAC Setup

NEW QUESTION 21

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 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		
🔍 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 22

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 26

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

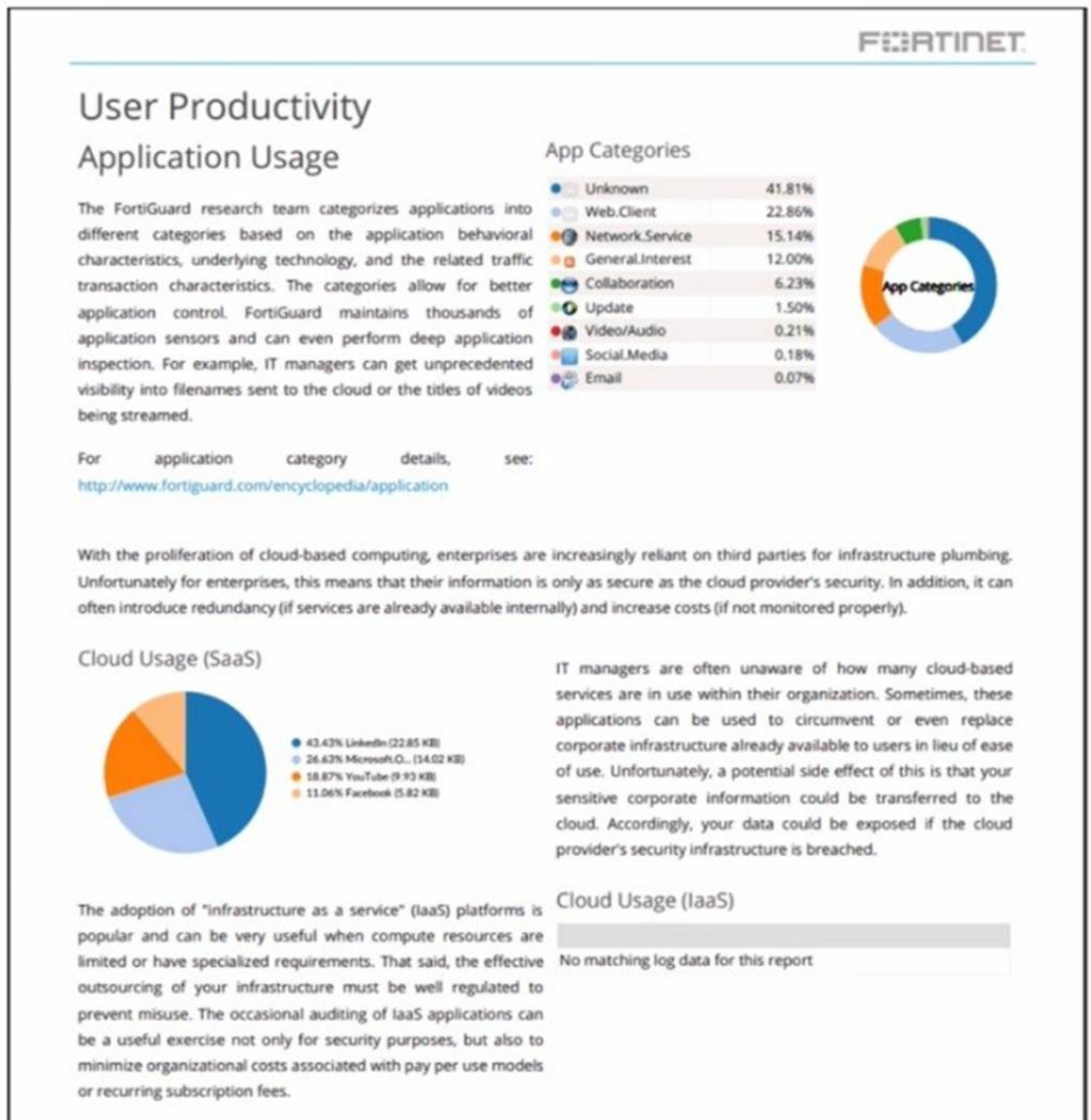
? FortiSASE Administration Guide - Configuring DEM

=====

NEW QUESTION 27

Refer to the exhibit.

Daily report for application usage



The daily report for application usage shows an unusually high number of unknown applications by category. What are two possible explanations for this? (Choose two.)

- A. Certificate inspection is not being used to scan application traffic.
- B. The inline-CASB application control profile does not have application categories set to Monitor
- C. Zero trust network access (ZTNA) tags are not being used to tag the correct users.
- D. Deep inspection is not being used to scan traffic.

Answer: BD

NEW QUESTION 28

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 32

.....

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