

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?

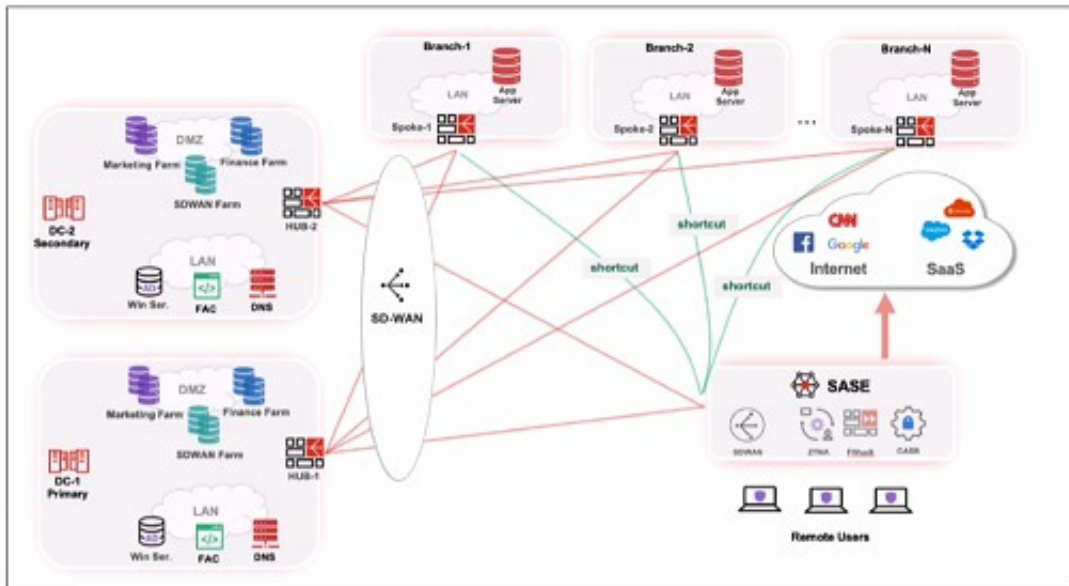
- A. 3
- B. 4
- C. 2
- D. 1

Answer: B

NEW QUESTION 2

Refer to the exhibits.

Topology



Priority settings

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

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 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 exhibits.

Web Filtering logs

	User	Destination P...	Traffic Type	Security Events	Security Action	Log Details
<input checked="" type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Details Security
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Category 50
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Category Description Information and Computer Security
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Direction outgoing
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Event Type ftgd_allow
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Hostname www.eicar.org
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Message URL belongs to an allowed category in policy
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Profile Group SIA (Internet Access)
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Referrer URI https://www.eicar.org/download-anti-malware-testfile/
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Request Type referral
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Sub Type webfilter
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Type utm
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	Timezone -0800
<input type="checkbox"/>	user2@fortinettraining.lab	443	Internet Access	Web Filter	Allowed	URL https://www.eicar.org/download/eicar_com-zip/?vpdmdl=8847&refresh=65df3477aha001709126775

Security Profile Group

The screenshot displays the FortiGate Security Fabric dashboard with four active security modules. At the top, there are 'Rename' and 'Delete' buttons. The modules are arranged in a 2x2 grid, each with a toggle switch and a 'Customize' button.

- AntiVirus:** Shows a list of inspected protocols with their counts and status.

Threats	Count	Inspected Protocols
		HTTP
		SMTP
		POP3
		IMAP
		FTP
		CIFS
- Web Filter With Inline-CASB:** Shows a list of filtered domains with their counts and filter status.

Threats	Count	Filters
www.eicar.org	80	Allow
5f3c395.com19.de	22	Block
www.eicar.com	19	Exempt
encrypted-tbn0.gstatic.com	9	Monitor
ocsp.digicert.com	8	Warning
		Disable
		Inline-CASB Headers
- Intrusion Prevention:** Shows the status of intrusion prevention.

Threats	Count	Intrusion Prevention
		Recommended Scanning traffic for all known threats and applying the recommended settings. Disabled
- SSL Inspection:** Shows the status of SSL inspection.

Threats	Count	SSL Inspection
ssl-anomaly	734	Deep Inspection SSL connections are decrypted to allow for inspection of the contents.
		Exempt Hosts
		Exempt URL Categories

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	<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 6

When accessing the FortiSASE portal for the first time, an administrator must select data center locations for which three FortiSASE components? (Choose three.)

- A. Endpoint management
- B. Points of presence
- C. SD-WAN hub
- D. Logging
- E. Authentication

Answer: ABD

Explanation:

When accessing the FortiSASE portal for the first time, an administrator must select data center locations for the following FortiSASE components:

? Endpoint Management:

? Points of Presence (PoPs):

? Logging:

References:

? FortiOS 7.2 Administration Guide: Details on initial setup and configuration steps for FortiSASE.

? FortiSASE 23.2 Documentation: Explains the importance of selecting data center locations for various FortiSASE components.

NEW QUESTION 7

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 8

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 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 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

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 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 12

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 13

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 18
Refer to the exhibits.

Secure private access service connection

Name	To_FortiGate	X
Remote Gateway	203.221.196.6	X
Authentication Method	<div>Pre-shared KeyCertificate</div>	
BGP Peer IP	10.11.11.1	X
Network Overlay ID	100	X

Secure private access network connection

Service Connections

Network Configuration

SECURE PRIVATE ACCESS NETWORK CONFIGURATION

BGP Routing Design

BGP per overlayBGP on loopback

BGP Router ID Subnet

10.12.11.0/24

×

Autonomous System Number (ASN)

65001

×

BGP Recursive Routing

☐

Hub Selection Method

Hub Health and PriorityBGP MED

Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.

i Within each PoP, the highest priority service connection that meets minimum SLA requirements is selected. Note that a service connection can be assigned a different priority level in different PoPs.

Health Check IP

10.1.0.254

×

Firewall policy configuration

```
config firewall policy
  edit 5
    set name "Spoke-to-Spoke"
    set uuid 4d949462-216b-51ee-03c7-d0662fdf9451
    set srcintf "To_SASE"
    set dstintf "To_SASE"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
    set comments "VPN: To_SASE (Created by VPN wizard)"
  next
  edit 6
    set name "Lo-BGP-HC"
    set uuid f5a12c92-216b-51ee-4802-80cd013d6acf
    set srcintf "To_SASE"
    set dstintf "SASE_Health"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
  next
  edit 9
    set name "Spoke-to-Hub"
    set uuid 617b81ee-cc64-51ee-8da6-6cdff3ca2cca
    set srcintf "To_SASE"
    set dstintf "internal3"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
  next
end
```

IPsec VPN configuration

```
# show vpn ipsec phase1-interface To_SASE
config vpn ipsec phase1-interface
  edit "To_SASE"
    set type dynamic
    set interface "wan1"
    set peertype any
    set net-device disable
    set mode-cfg enable
    set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
    set add-route disable
    set dpd on-idle
    set comments "VPN: To_SASE (Created by VPN wizard)"
    set wizard-type hub-fortigate-auto-discovery
    set auto-discovery-sender enable
    set ipv4-start-ip 10.11.11.10
    set ipv4-end-ip 10.11.11.200
    set ipv4-netmask 255.255.255.0
    set unity-support disable
    set psksecret ENC Sbl0igpvIFFYSpRZ/hyxQVUXv9NZm7uqltD9v+BViPd+7RWizmUA3ZINn0zbsxq70FiYkPLkxanWIo7VLiipkye1xt84NAwEf_m5jTqqf1dMj/phYvBI3hzU0yXq==
  next
end

# show vpn ipsec phase2-interface To_SASE
config vpn ipsec phase2-interface
  edit "To_SASE"
    set phase1name "To_SASE"
    set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
    set comments "VPN: To_SASE (Created by VPN wizard)"
  next
end
```

BGP protocol configuration

```
#config router bgp
  set as 65001
  set router-id 10.1.0.254
  config neighbor
    edit "10.10.1.3"
      set advertisement-interval 1
      set ebgp-enforce-multihop enable
      set link-down-failover enable
      set remote-as 65001
      set route-reflector-client enable
    next
  end
  config neighbor-group
    edit "To_SASE"
      set capability-graceful-restart enable
      set link-down-failover enable
      set next-hop-self enable
      set interface "To_SASE"
      set remote-as 65001
      set additional-path both
      set adv-additional-path 4
      set route-reflector-client enable
    next
  end
  config neighbor-range
    edit 1
      set prefix 10.11.11.0 255.255.255.0
      set neighbor-group "To_SASE"
    next
  end
  config network
    edit 1
      set prefix 10.190.190.0 255.255.255.0
    next
  end
```

A FortiSASE administrator is trying to configure FortiSASE as a spoke to a FortiGate hub. The VPN tunnel does not establish. Based on the provided configuration, what configuration needs to be modified to bring the tunnel up?

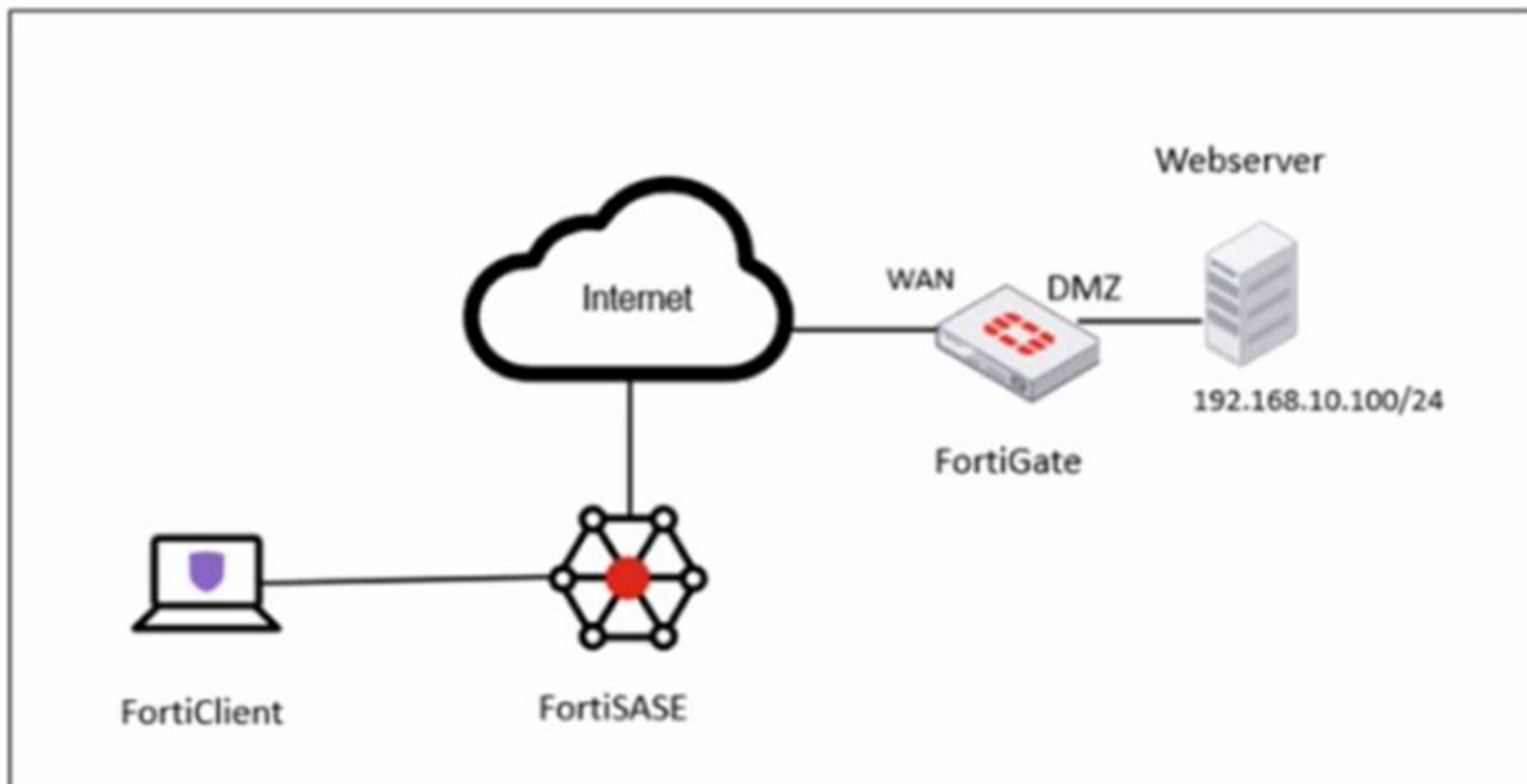
- A. NAT needs to be enabled in the Spoke-to-Hub firewall policy.
- B. The BGP router ID needs to match on the hub and FortiSASE.
- C. FortiSASE spoke devices do not support mode config.
- D. The hub needs IKEv2 enabled in the IPsec phase 1 settings.

Answer: D

NEW QUESTION 23

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

AllVPN UsersEdge Device

Source

All TrafficSpecify

User

All VPN UsersSpecify

Destination

Private Access TrafficSpecify

Service

ALL_ICMP

+

×

Profile Group

DefaultSpecify

Force Certificate Inspection ⓘ

☐

Action

✓ Accept

⊘ Deny

Status

✔ Enable

✖ Disable

Logging Options

Log Allowed Traffic ☒

Security EventsAll 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 28

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 32

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

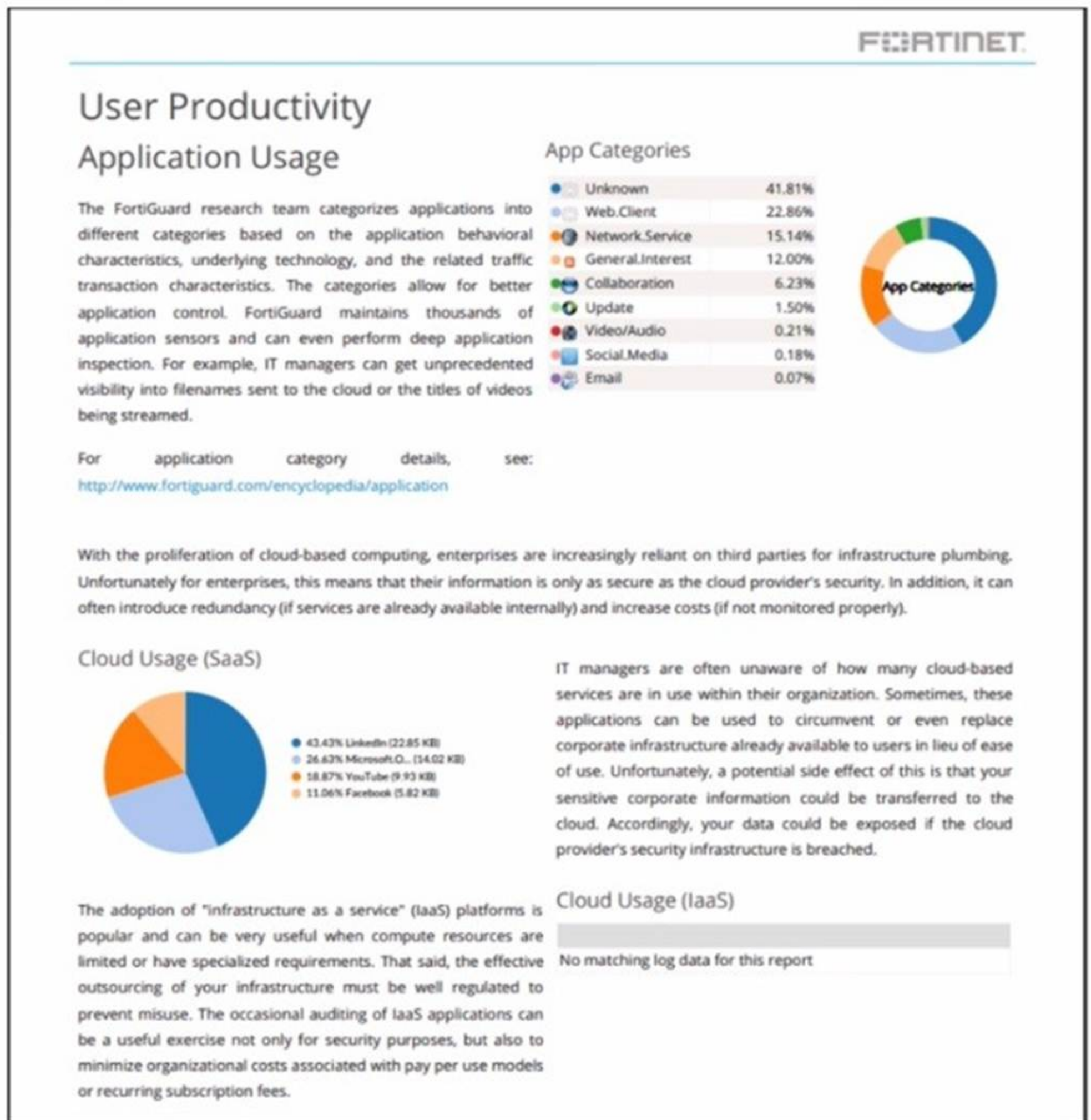
? FortiSASE Administration Guide - Configuring DEM

=====

NEW QUESTION 35

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 36

A customer wants to upgrade their legacy on-premises proxy to a cloud-based proxy for a hybrid network. Which FortiSASE features would help the customer to achieve this outcome?

- A. SD-WAN and NGFW
- B. SD-WAN and inline-CASB
- C. zero trust network access (ZTNA) and next generation firewall (NGFW)
- D. secure web gateway (SWG) and inline-CASB

Answer: D

Explanation:

For a customer looking to upgrade their legacy on-premises proxy to a cloud- based proxy for a hybrid network, the combination of Secure Web Gateway (SWG) and Inline Cloud Access Security Broker (CASB) features in FortiSASE will provide the necessary capabilities.

? Secure Web Gateway (SWG):

? Inline Cloud Access Security Broker (CASB):

References:

? FortiOS 7.2 Administration Guide: Details on SWG and CASB features.

? FortiSASE 23.2 Documentation: Explains how SWG and inline-CASB are used in cloud-based proxy solutions.

NEW QUESTION 37

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 40

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 45

.....

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