

Fortinet

Exam Questions FCSS_SASE_AD-24

FCSS - FortiSASE 24 Administrator



NEW QUESTION 1

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

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

Answer: B

Explanation:

If the daily summary report generated by FortiSASE contains very little data, one possible explanation is that the "Log allowed traffic" setting is configured to log only "Security Events" for all policies. This configuration limits the amount of data logged, as it only includes security events and excludes normal allowed traffic.

? Log Allowed Traffic Setting:

? Impact on Report Data:

References:

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

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

NEW QUESTION 2

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

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

Answer: BCD

Explanation:

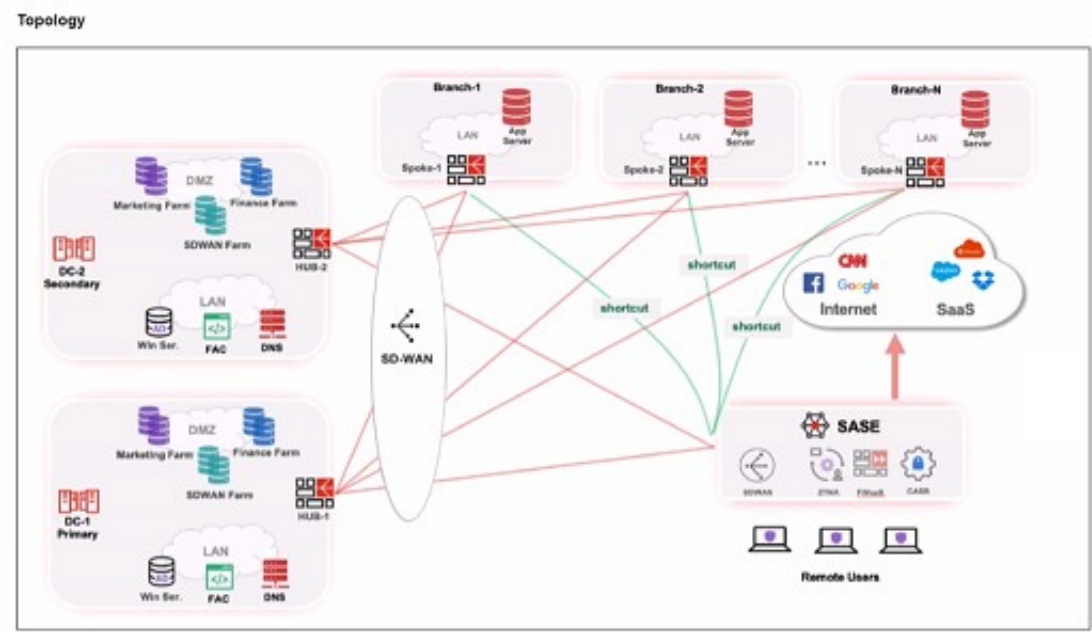
References:

? FortiOS 7.2 Administration Guide: Provides details on configuring Secure Private Access and integrating with FortiGate.

? FortiSASE 23.2 Documentation: Explains how to set up and manage connections between FortiSASE and corporate FortiGate.

NEW QUESTION 3

Refer to the exhibits.



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	

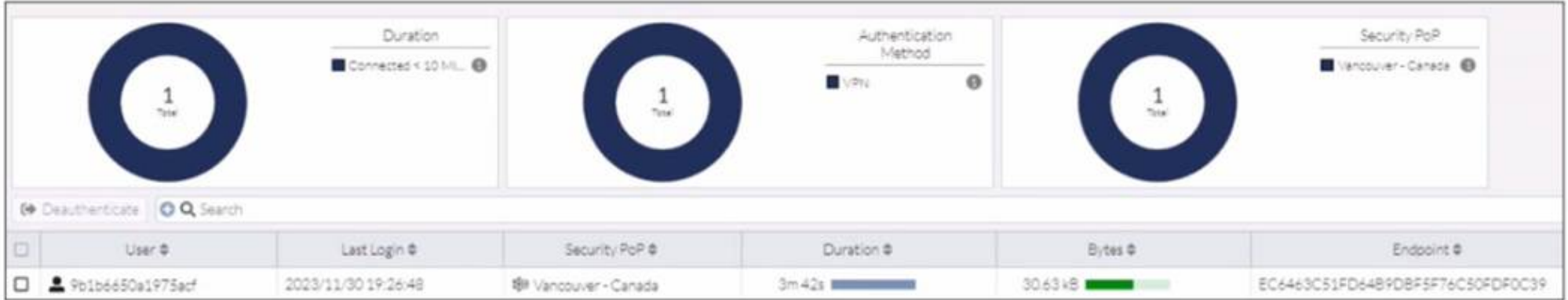
When remote users connected to FortiSASE require access to internal resources on Branch-2. how will traffic be routed?

- 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

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 information in 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 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/?wpdmdl=8847&refresh=65df3477aha001709126775

Security Profile Group

Rename

Delete

AntiVirus

Threats

Count

Inspected Protocols

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

9

Warning

0

Disable

0

Inline-CASB Headers

1

View All

View Logs

Customize

Intrusion Prevention

Threats

Count

Intrusion Prevention

Recommended

Scanning traffic for all known threats and applying the recommended settings.

Disabled

View All

View Logs

Customize

SSL Inspection

Threats

Count

SSL Inspection

ssl-anomaly

734

Deep Inspection

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

4 Exempt Hosts

1

Exempt URL Categories

2

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 +
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

Which role does FortiSASE play in supporting zero trust network access (ZTNA) principles?

- 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 7

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 8

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 9

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 10

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

- A. The security posture of the device is secure.

- B. All FortiSASE user-based deployments are supported.
- C. All TCP-based applications are supported.
- D. Data center redundancy is offered.

Answer: AC

Explanation:

Zero Trust Network Access (ZTNA) private access use cases focus on providing secure and controlled access to private applications without exposing them to the public internet. The following two statements accurately describe ZTNA private access use cases:

? The security posture of the device is secure (Option A):ZTNA enforces strict access controls based on the principle of least privilege. Before granting access to private applications, ZTNA evaluates the security posture of the device (e.g., whether it is patched, compliant, and free of malware). Only devices that meet the required security standards are granted access, ensuring that the device is secure

before allowing private access.

? All TCP-based applications are supported (Option C):ZTNA supports all TCP- based applications, enabling secure access to a wide range of private applications, including legacy systems and custom-built applications. This flexibility makes ZTNA suitable for organizations with diverse application environments.

Here??s why the other options are incorrect:

? B. All FortiSASE user-based deployments are supported:While FortiSASE supports various deployment scenarios, not all user-based deployments are automatically compatible with ZTNA. Specific configurations and requirements must be met to enable ZTNA functionality.

? D. Data center redundancy is offered:Data center redundancy is unrelated to ZTNA private access use cases. Redundancy typically pertains to infrastructure design and failover mechanisms, not access control methodologies like ZTNA.

References:

? Fortinet FCSS FortiSASE Documentation - ZTNA Private Access Overview

? FortiSASE Administration Guide - ZTNA Deployment Best Practices

NEW QUESTION 10

Which event log subtype captures FortiSASE SSL VPN user creation?

- A. Endpoint Events
- B. VPN Events
- C. User Events
- D. Administrator Events

Answer: C

Explanation:

Theevent log subtypethat captures FortiSASE SSL VPN user creation is User Events. This subtype is specifically designed to log activities related to user management, such as creating, modifying, or deleting user accounts. When an SSL VPN user is created, it falls under this category because it involves adding a new user to the system.

Here??s why the other options are incorrect:

? A. Endpoint Events:These logs pertain to activities related to endpoint devices, such as device registration, compliance checks, or security posture assessments. SSL VPN user creation is unrelated to endpoint events.

? B. VPN Events:These logs capture activities related to VPN connections, such as session establishment, termination, or errors. While SSL VPN usage generates VPN events, the creation of a user account itself is not logged under this subtype.

? D. Administrator Events:These logs track actions performed by administrators, such as configuration changes or policy updates. While an administrator might create the SSL VPN user, the specific event of user creation is categorized under User Events, not Administrator Events.

References:

? Fortinet FCSS FortiSASE Documentation - Event Logging and Subtypes

? FortiSASE Administration Guide - Monitoring and Logging

NEW QUESTION 11

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:

TheFortiGuard forensics analysis featureon FortiSASE is designed to help customersidentify 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 16

Refer to the exhibits.

Secure private access service connection

Name	<input type="text" value="To_FortiGate"/>	X
Remote Gateway	<input type="text" value="203.221.196.6"/>	X
Authentication Method	<input type="radio"/> Pre-shared Key <input type="radio"/> Certificate	
BGP Peer IP	<input type="text" value="10.11.11.1"/>	X
Network Overlay ID	<input type="text" value="100"/>	X

Secure private access network connection

Service Connections
Network Configuration

SECURE PRIVATE ACCESS NETWORK CONFIGURATION

BGP Routing Design	<input type="radio"/> BGP per overlay <input type="radio"/> BGP on loopback
BGP Router ID Subnet	<input type="text" value="10.12.11.0/24"/> X
Autonomous System Number (ASN)	<input type="text" value="65001"/> X
BGP Recursive Routing	<input type="checkbox"/>
Hub Selection Method	<input type="radio"/> Hub Health and Priority <input type="radio"/> BGP 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	<input type="text" value="10.1.0.254"/> X
-----------------	---

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+7RWizmUA3ZINn0zbsxq70F
iYkPLkxanWIo7VLiipkye1xt84NAwEfm5jTqqf1dMj/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 19

Refer to the exhibit.

Security Logs

Log Details

Destination

Destination IP

151.101.40.81


Destination Port

443

Destination Country/Region

United States

Traffic Type

 Internet Access

Destination UUID

4a501662-f85f-51ed-5194-7e45b3d369cd

Hostname

www.bbc.com


URL

https://www.bbc.com/

Application Control

Action

Action

 Blocked

Threat

16,777,216

Policy ID

8

Policy UUID

7d56f000-b41e-51ee-f96b-d0b4d9fb3c2b

Policy Type

policy

Security

Web Filter

Profile Group

 SIA (Internet Access)

Request Type

direct

Direction

incoming

Banned Word

fight

Message

URL was blocked because it contained banned word(s).

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

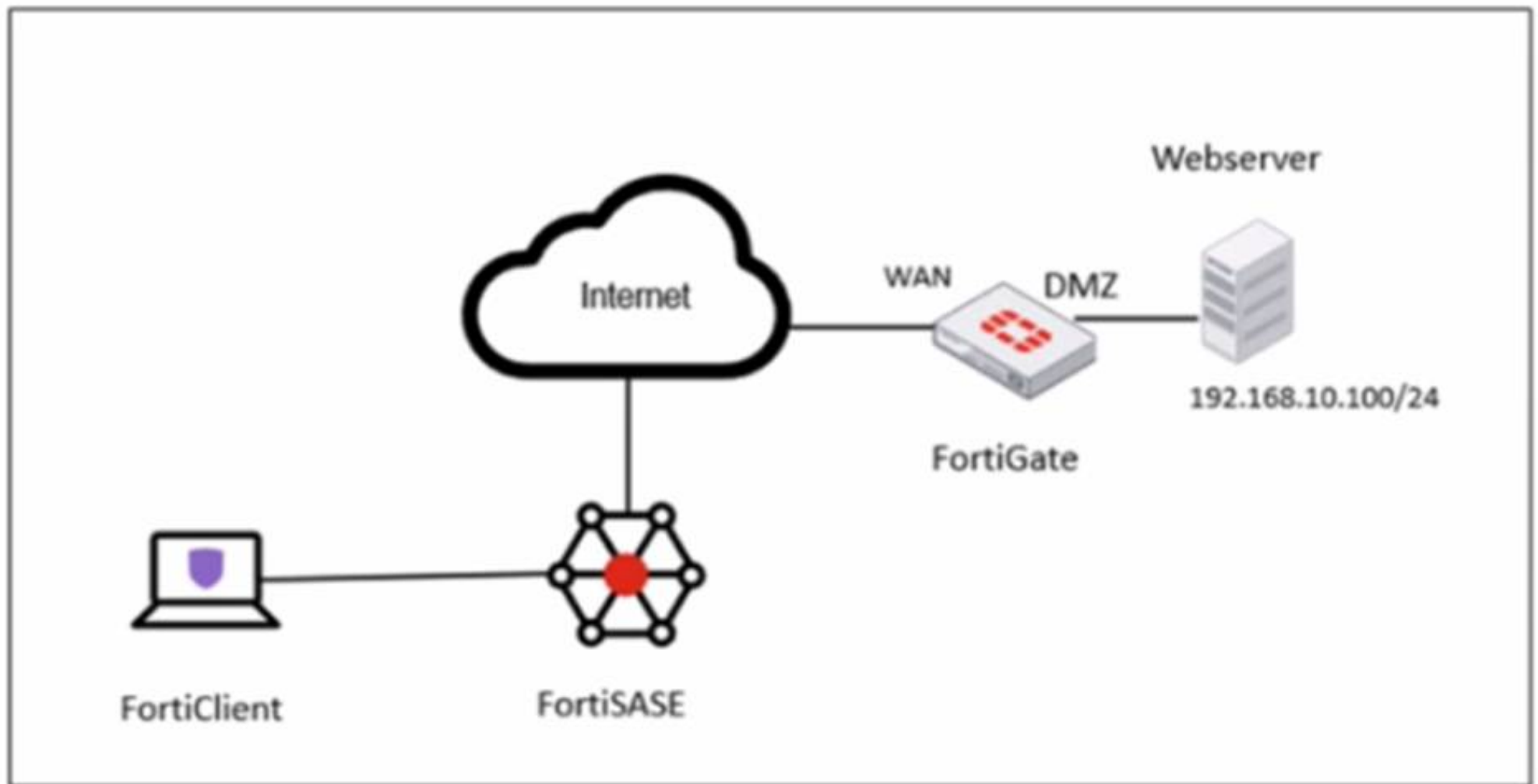
- A. FortiGuard category-based filter
- B. content filter
- C. URL Filter
- D. inline cloud access security broker (CASB) headers

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=42025/00 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 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 27

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

+ Create	Edit	Delete	<input type="text" value="Search"/>			
<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 28

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 30

What are two advantages of using zero-trust tags? (Choose two.)

- A. Zero-trust tags can be used to allow or deny access to network resources
- B. Zero-trust tags can determine the security posture of an endpoint.

- C. Zero-trust tags can be used to create multiple endpoint profiles which can be applied to different endpoints
 D. Zero-trust tags can be used to allow secure web gateway (SWG) access

Answer: AB

Explanation:

Zero-trust tags are critical in implementing zero-trust network access (ZTNA) policies. Here are the two key advantages of using zero-trust tags:

? Access Control (Allow or Deny):

? Determining Security Posture:

References:

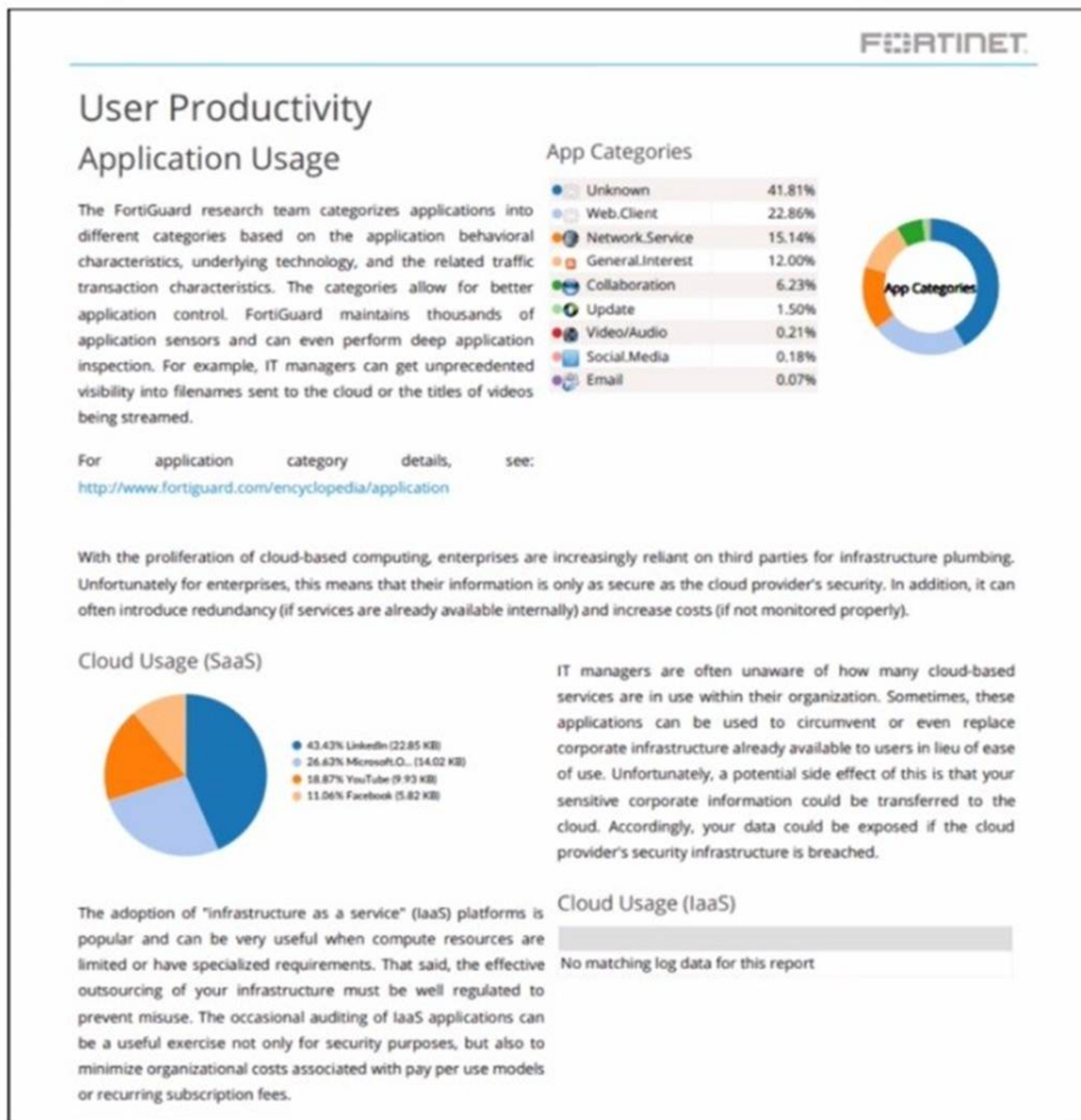
? FortiOS 7.2 Administration Guide: Provides detailed information on configuring and using zero-trust tags for access control and security posture assessment.

? FortiSASE 23.2 Documentation: Explains how zero-trust tags are implemented and used within the FortiSASE environment for enhancing security and compliance.

NEW QUESTION 32

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 37

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 42

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_SASE_AD-24 Practice Test Here](#)