

Fortinet

Exam Questions FCSS_SASE_AD-23

FCSS FortiSASE 23 Administrator



NEW QUESTION 1

Which secure internet access (SIA) use case minimizes individual workstation or device setup, because you do not need to install FortiClient on endpoints or configure explicit web proxy settings on web browser-based endpoints?

- A. SIA for inline-CASB users
- B. SIA for agentless remote users
- C. SIA for SSLVPN remote users
- D. SIA for site-based remote users

Answer: B

Explanation:

The Secure Internet Access (SIA) use case that minimizes individual workstation or device setup is SIA for agentless remote users. This use case does not require installing FortiClient on endpoints or configuring explicit web proxy settings on web browser-based endpoints, making it the simplest and most efficient deployment.

? SIA for Agentless Remote Users:

? Minimized Setup:

References:

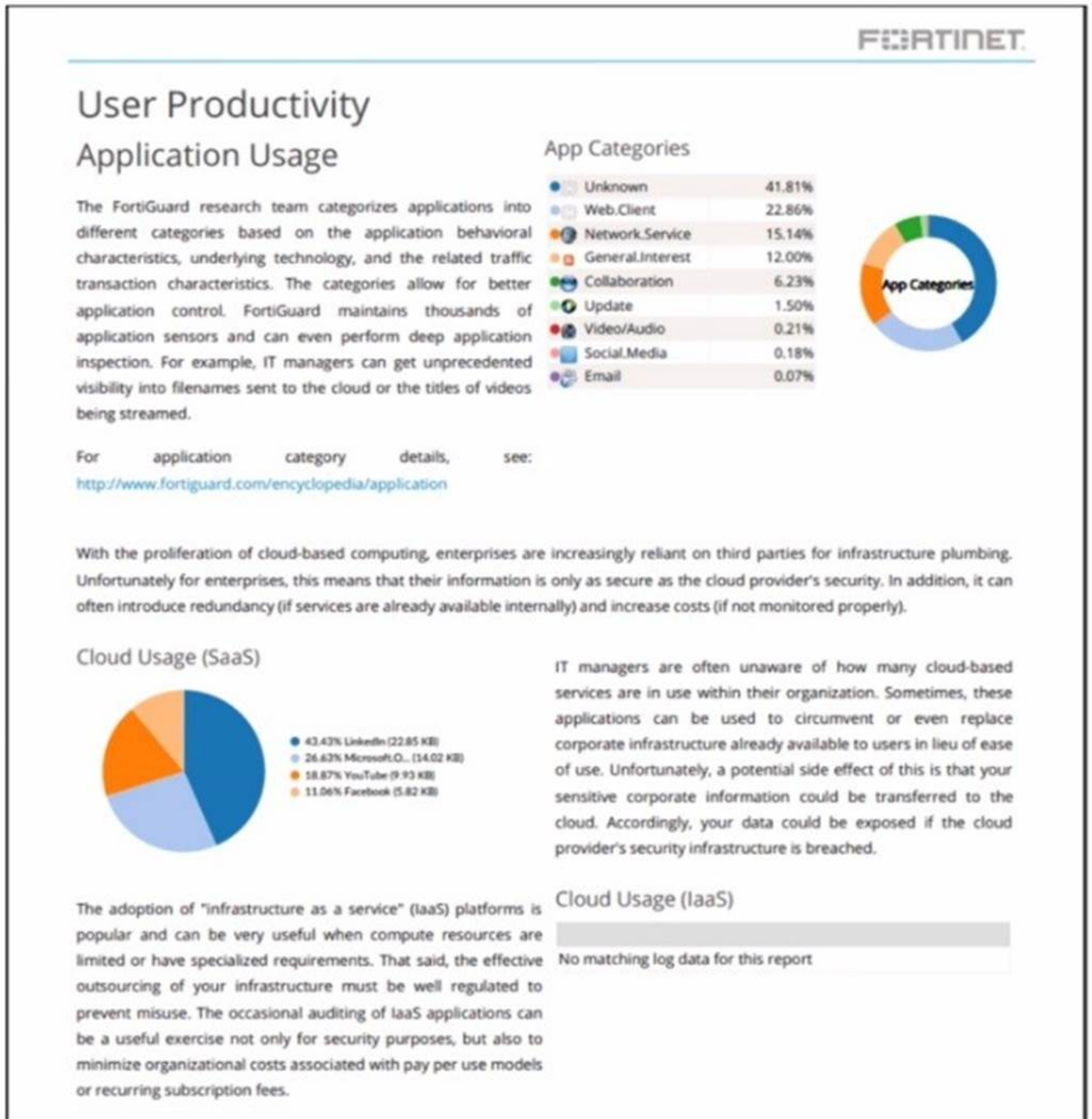
? FortiOS 7.2 Administration Guide: Details on different SIA deployment use cases and configurations.

? FortiSASE 23.2 Documentation: Explains how SIA for agentless remote users is implemented and the benefits it provides.

NEW QUESTION 2

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: AD

Explanation:

The unusually high number of unknown applications by category in the daily report for application usage can be attributed to the following reasons:

? Certificate Inspection is not being used to scan application traffic:

? Deep Inspection is not being used to scan traffic:

References:

? FortiOS 7.2 Administration Guide: Details on certificate inspection and deep inspection configurations.

? FortiSASE 23.2 Documentation: Explains the importance of deep inspection and certificate inspection in accurate application identification.

NEW QUESTION 3

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: D

Explanation:

During FortiSASE provisioning, the FortiSASE administrator needs to configure at least one security point of presence (PoP). A single PoP is sufficient to get started with FortiSASE, providing the necessary security services and connectivity for users.

? Security Point of Presence (PoP):

? Scalability:

References:

? FortiOS 7.2 Administration Guide: Provides details on the provisioning process for FortiSASE.

? FortiSASE 23.2 Documentation: Explains the configuration and role of security PoPs in the FortiSASE architecture.

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

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 6

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

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

Answer: BD

Explanation:

FortiSASE uses the following components for application control to act as an inline-CASB (Cloud Access Security Broker):

? SSL Deep Inspection:

? Web Filter with Inline-CASB:

References:

? FortiOS 7.2 Administration Guide: Details on SSL deep inspection and web filtering configurations.

? FortiSASE 23.2 Documentation: Explains how FortiSASE acts as an inline-CASB using SSL deep inspection and web filtering.

NEW QUESTION 7

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 8

An organization wants to block all video and audio application traffic but grant access to videos from CNN Which application override action must you configure in the Application Control with Inline-CASB?

- A. Allow
- B. Pass
- C. Permit
- D. Exempt

Answer: D

Explanation:

? Application Control Configuration:

? Blocking Video and Audio Applications:

? Granting Access to Specific Videos (CNN):

? Configuration Steps:

References:

? FortiOS 7.2 Administration Guide: Detailed steps on configuring Application Control and Inline-CASB.

? Fortinet Training Institute: Provides scenarios and examples of using Application Control with Inline-CASB for specific use cases.

NEW QUESTION 9

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: BC

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 10

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: ABD

Explanation:

When deploying FortiSASE agent-based clients, several features are available that are not typically available with an agentless solution. These features enhance the security and management capabilities for endpoints.

? Vulnerability Scan:

? SSL Inspection:

? Web Filter:

References:

? FortiOS 7.2 Administration Guide: Explains the features and benefits of deploying agent-based clients.

? FortiSASE 23.2 Documentation: Details the differences between agent-based and agentless solutions and the additional features provided by agent-based deployments.

NEW QUESTION 10

Which two advantages does FortiSASE bring to businesses with multiple branch offices? (Choose two.)

- A. It offers centralized management for simplified administration.

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

Answer: AD

Explanation:

FortiSASE brings the following advantages to businesses with multiple branch offices:

? Centralized Management for Simplified Administration:

? Eliminates the Need for On-Premises Firewalls:

References:

? FortiOS 7.2 Administration Guide: Provides information on the benefits of centralized management and cloud-based security solutions.

? FortiSASE 23.2 Documentation: Explains the advantages of using FortiSASE for businesses with multiple branch offices, including reduced need for on-premises firewalls.

NEW QUESTION 15

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: ABC

Explanation:

To configure a Secure Private Access (SPA) solution to share endpoint information between FortiSASE and a corporate FortiGate, you need to take the following steps:

? Add the FortiGate IP address in the secure private access configuration on

FortiSASE:

? Use the FortiClient EMS cloud connector on the corporate FortiGate to connect to FortiSASE:

? Register FortiGate and FortiSASE under the same FortiCloud account:

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 20

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 filter 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: C

Explanation:

The exhibit indicates that the URL <https://www.bbc.com/is> is being blocked due to containing a banned word ("fight"). To allow access to this specific URL, you need to adjust the URL filter settings on FortiSASE.

? URL Filtering:

? Modifying URL Filter:

References:

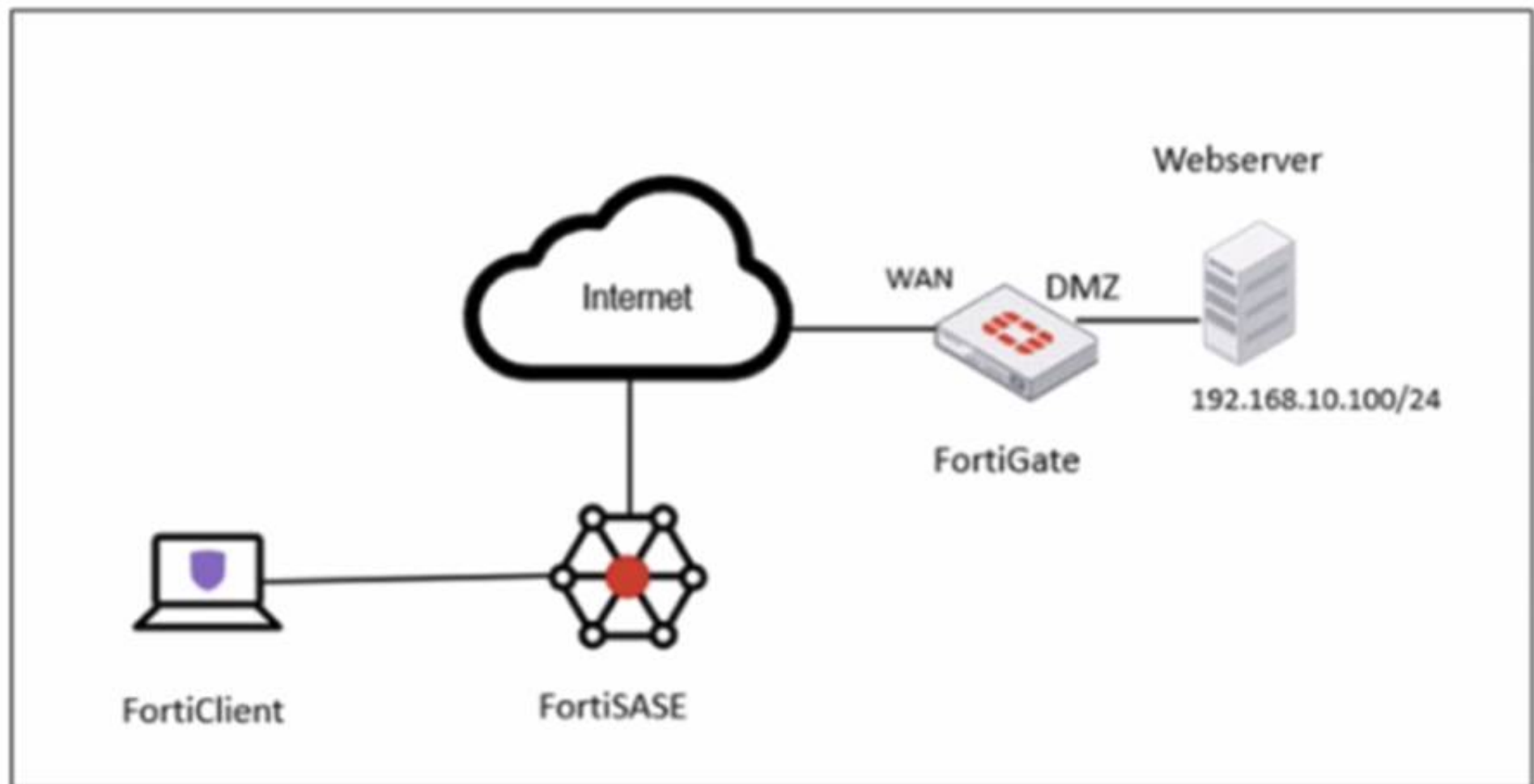
? FortiOS 7.2 Administration Guide: Provides details on configuring and managing URL filters.

? FortiSASE 23.2 Documentation: Explains how to set up and modify web filtering policies, including URL filters.

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 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	<input type="checkbox"/>
Action	Accept Deny
Status	Enable Disable
Logging Options	
Log Allowed Traffic	<input type="checkbox"/> Security Events All Sessions

BGP route information on FortiSASE

Learned BGP Routes		
<div><div></div><div>Search</div></div>		
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: B

Explanation:

The reason for the ping failures is due to the quick mode selectors restricting the subnet. Quick mode selectors define the IP ranges and protocols that are allowed through the VPN tunnel, and if they are not configured correctly, traffic to certain subnets can be blocked.

? Quick Mode Selectors:

? Diagnostic Output:

? Configuration Check:

References:

- ? FortiOS 7.2 Administration Guide: Provides detailed information on configuring VPN tunnels and quick mode selectors.
- ? FortiSASE 23.2 Documentation: Explains how to set up and manage VPN tunnels, including the configuration of quick mode selectors.

NEW QUESTION 27

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 30

.....

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-23 Practice Exam Features:

- * FCSS_SASE_AD-23 Questions and Answers Updated Frequently
- * FCSS_SASE_AD-23 Practice Questions Verified by Expert Senior Certified Staff
- * FCSS_SASE_AD-23 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCSS_SASE_AD-23 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCSS_SASE_AD-23 Practice Test Here](#)