

Fortinet

Exam Questions FCSS_SASE_AD-23

FCSS FortiSASE 23 Administrator



NEW QUESTION 1

To complete their day-to-day operations, remote users require access to a TCP-based application that is hosted on a private web server. Which FortiSASE deployment use case provides the most efficient and secure method for meeting the remote users' requirements?

- A. SD-WAN private access
- B. inline-CASB
- C. zero trust network access (ZTNA) private access
- D. next generation firewall (NGFW)

Answer: C

Explanation:

Zero Trust Network Access (ZTNA) private access provides the most efficient and secure method for remote users to access a TCP-based application hosted on a private web server. ZTNA ensures that only authenticated and authorized users can access specific applications based on predefined policies, enhancing security and access control.

? Zero Trust Network Access (ZTNA):

? Secure and Efficient Access:

References:

? FortiOS 7.2 Administration Guide: Provides detailed information on ZTNA and its deployment use cases.

? FortiSASE 23.2 Documentation: Explains how ZTNA can be used to provide secure access to private applications for remote users.

NEW QUESTION 2

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 3

Refer to the exhibit.

Daily report for application usage

FORTINET.

User Productivity Application Usage

The FortiGuard research team categorizes applications into different categories based on the application behavioral characteristics, underlying technology, and the related traffic transaction characteristics. The categories allow for better application control. FortiGuard maintains thousands of application sensors and can even perform deep application inspection. For example, IT managers can get unprecedented visibility into filenames sent to the cloud or the titles of videos being streamed.

For application category details, see: <http://www.fortiguard.com/encyclopedia/application>

With the proliferation of cloud-based computing, enterprises are increasingly reliant on third parties for infrastructure plumbing. Unfortunately for enterprises, this means that their information is only as secure as the cloud provider's security. In addition, it can often introduce redundancy (if services are already available internally) and increase costs (if not monitored properly).

App Categories

Unknown	41.81%
Web.Client	22.86%
Network.Service	15.14%
General.Interest	12.00%
Collaboration	6.23%
Update	1.50%
Video/Audio	0.21%
Social.Media	0.18%
Email	0.07%



Cloud Usage (SaaS)



- 43.43% LinkedIn (22.85 KB)
- 26.63% Microsoft.O... (14.02 KB)
- 18.87% YouTube (9.93 KB)
- 11.06% Facebook (5.82 KB)

IT managers are often unaware of how many cloud-based services are in use within their organization. Sometimes, these applications can be used to circumvent or even replace corporate infrastructure already available to users in lieu of ease of use. Unfortunately, a potential side effect of this is that your sensitive corporate information could be transferred to the cloud. Accordingly, your data could be exposed if the cloud provider's security infrastructure is breached.

Cloud Usage (IaaS)

No matching log data for this report

The adoption of "infrastructure as a service" (IaaS) platforms is popular and can be very useful when compute resources are limited or have specialized requirements. That said, the effective outsourcing of your infrastructure must be well regulated to prevent misuse. The occasional auditing of IaaS applications can be a useful exercise not only for security purposes, but also to minimize organizational costs associated with pay per use models or recurring subscription fees.

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 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.



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 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

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 8

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 9

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 10

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

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	9	Warning 0
		Disable 0
		Inline-CASB Headers 1

View All
View Logs
Customize

Intrusion Prevention
ⓘ

Threats	Count	Intrusion Prevention
		<div style="border: 1px solid #ccc; padding: 5px; margin: 5px;"> <p style="margin: 0;">Recommended</p> <p style="margin: 0;">Scanning traffic for all known threats and applying the recommended settings.</p> <p style="text-align: center; margin: 0;">Disabled</p> </div>

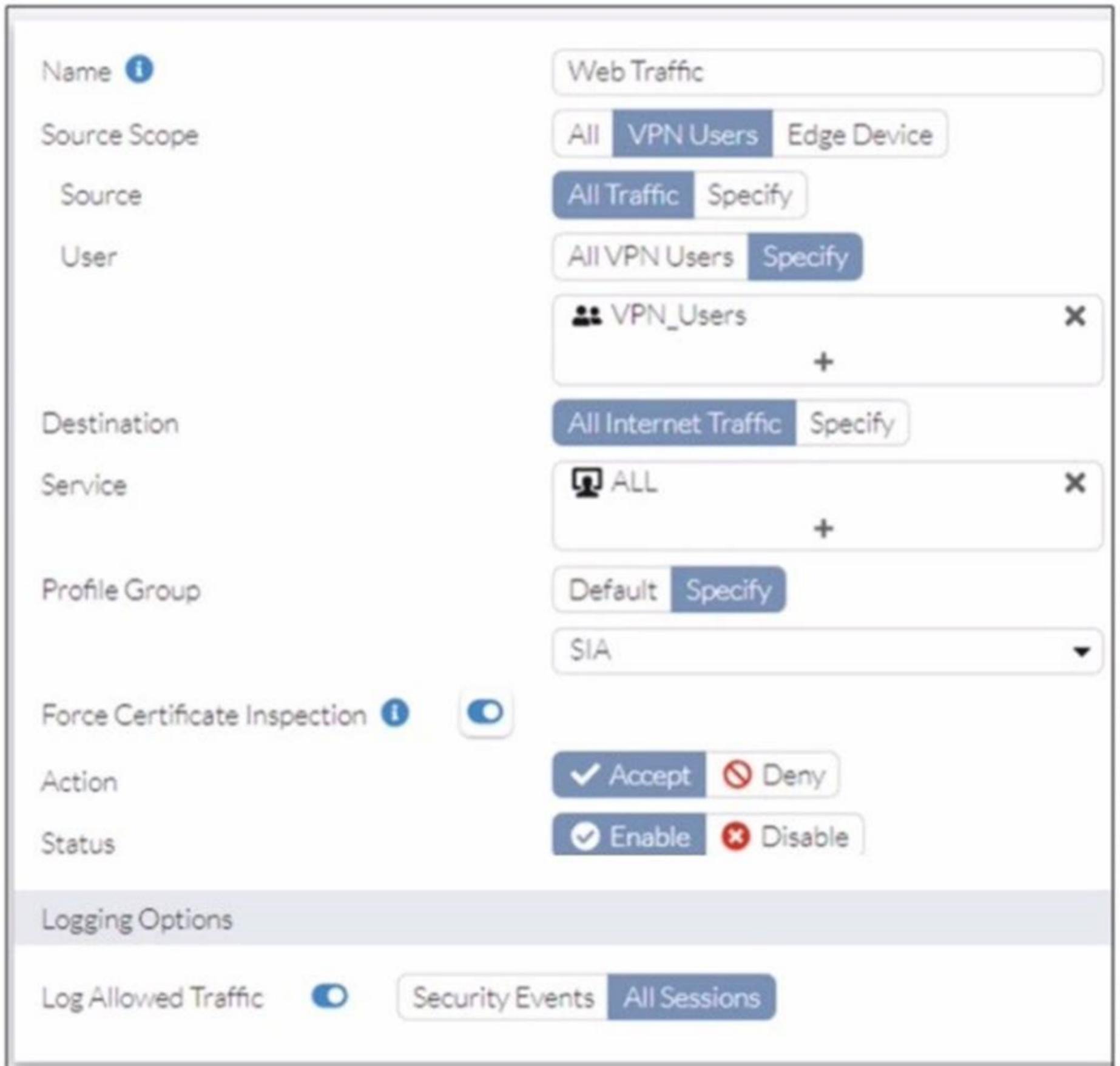
View All
View Logs
Customize

SSL Inspection
ⓘ

Threats	Count	SSL Inspection
ssl-anomaly	734	<p>Deep Inspection</p> <ul style="list-style-type: none"> 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



The screenshot shows the configuration for a Secure Internet Access policy named "Web Traffic".

- Name:** Web Traffic
- Source Scope:** All, VPN Users (selected), Edge Device
- Source:** All Traffic (selected), Specify
- User:** All VPN Users, Specify
- User Selection:** VPN_Users (selected), +
- Destination:** All Internet Traffic (selected), Specify
- Service:** ALL (selected), +
- Profile Group:** Default, Specify
- Profile Group Selection:** SIA (selected), ▾
- Force Certificate Inspection:** (enabled)
- Action:** Accept, Deny
- Status:** Enable, Disable
- Logging Options:**
 - Log Allowed Traffic:** (enabled)
 - Logging Selection:** Security Events, All Sessions (selected)

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: A

Explanation:

? Web Filtering Logs Analysis:

? Security Profile Group Configuration:

? Antivirus Profile Configuration:

? Policy Configuration:

References:

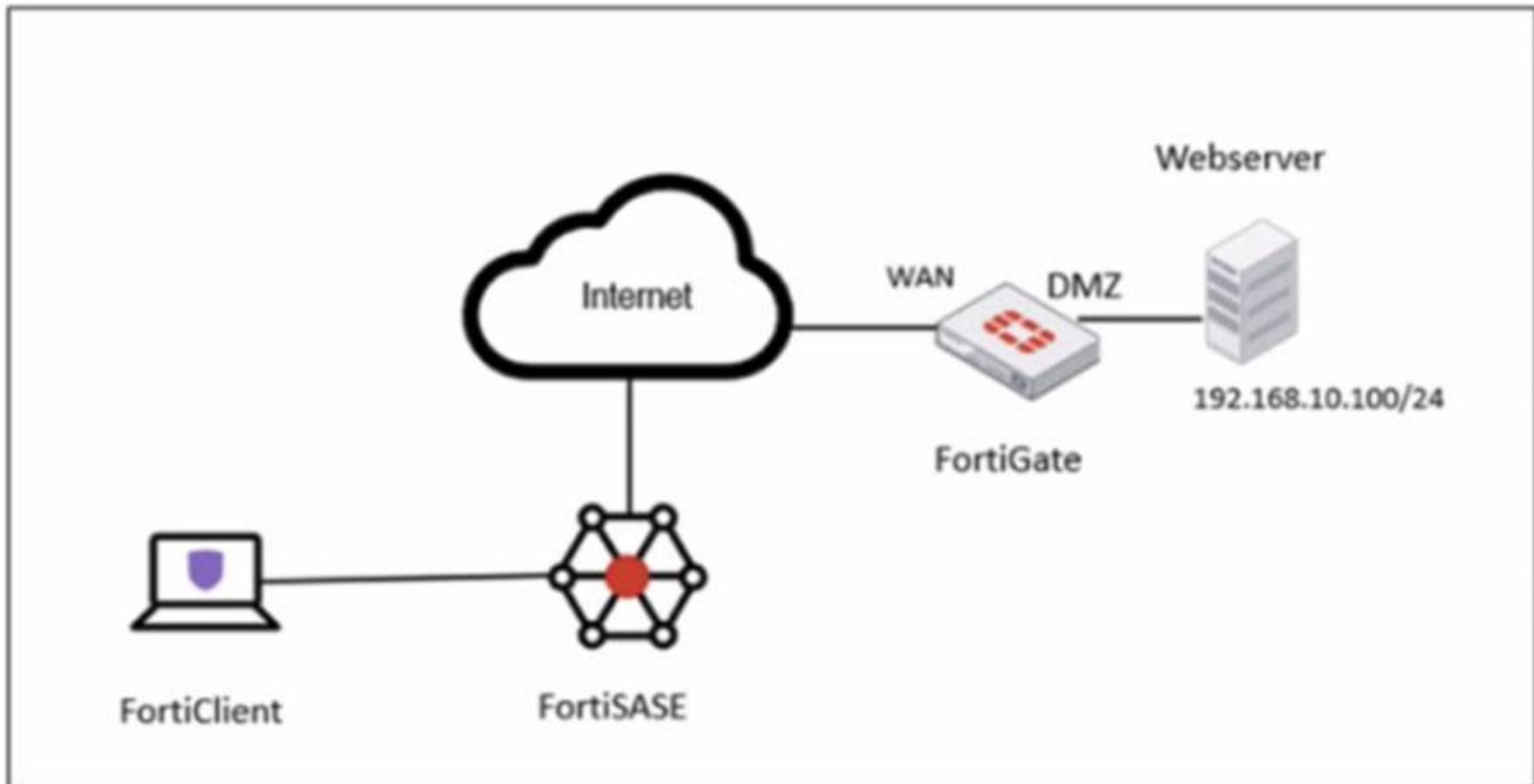
? FortiGate Security 7.2 Study Guide: Provides details on the precedence of web filtering over antivirus in security profiles.

? Fortinet Knowledge Base: Detailed explanation of web filtering and antivirus profiles interaction.

NEW QUESTION 10

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 ⓘ

Source Scope All VPN Users Edge Device

Source All Traffic Specify

User All VPN Users Specify

Destination Private Access Traffic Specify

Service + ×

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

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 12

.....

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](#)