Exam Questions FCSS_SASE_AD-23

FCSS FortiSASE 23 Administrator

https://www.2passeasy.com/dumps/FCSS_SASE_AD-23/

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

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

Answer: B

Explanation:
FortiSASE hides user information when viewing and analyzing logs by hashing data using salt. This approach ensures that sensitive user information is obfuscated, enhancing privacy and security.
? Hashing Data with Salt:
? Security and Privacy:
References:
? FortiOS 7.2 Administration Guide: Provides information on log management and data protection techniques.
? FortiSASE 23.2 Documentation: Details on how FortiSASE implements data hashing and salting to secure user information in logs.

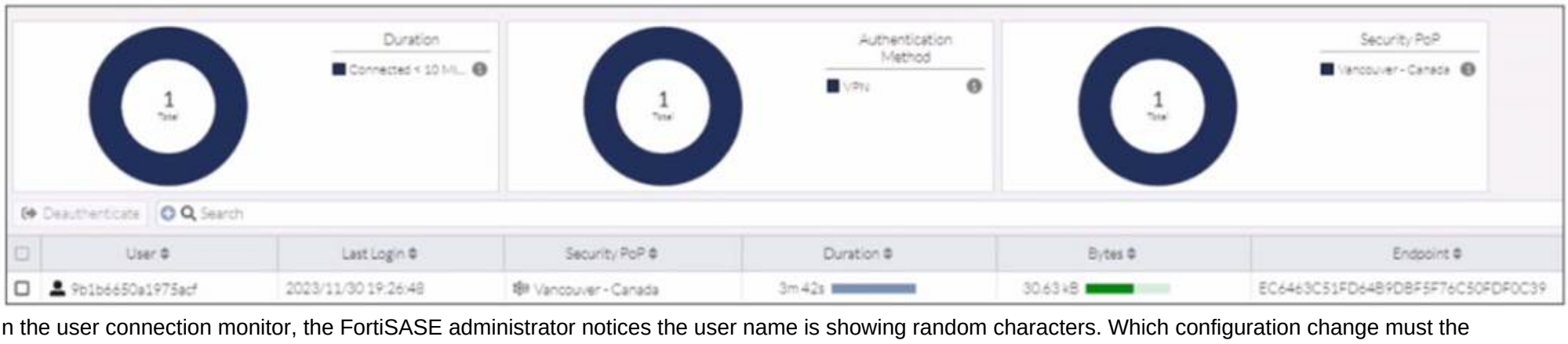
NEW QUESTION 3
Which two components are part of onboarding a secure web gateway (SWG) endpoint? (Choose two)

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 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.

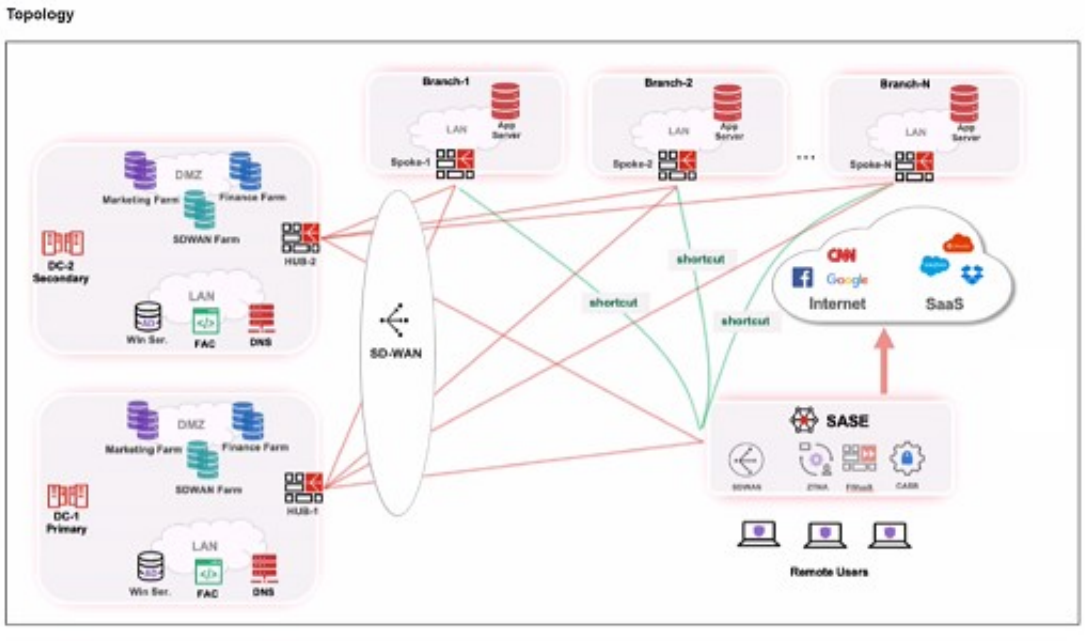
NEW QUESTION 5
Which two additional components does FortiSASE use for application control to act as an inline-CASB? (Choose two.)

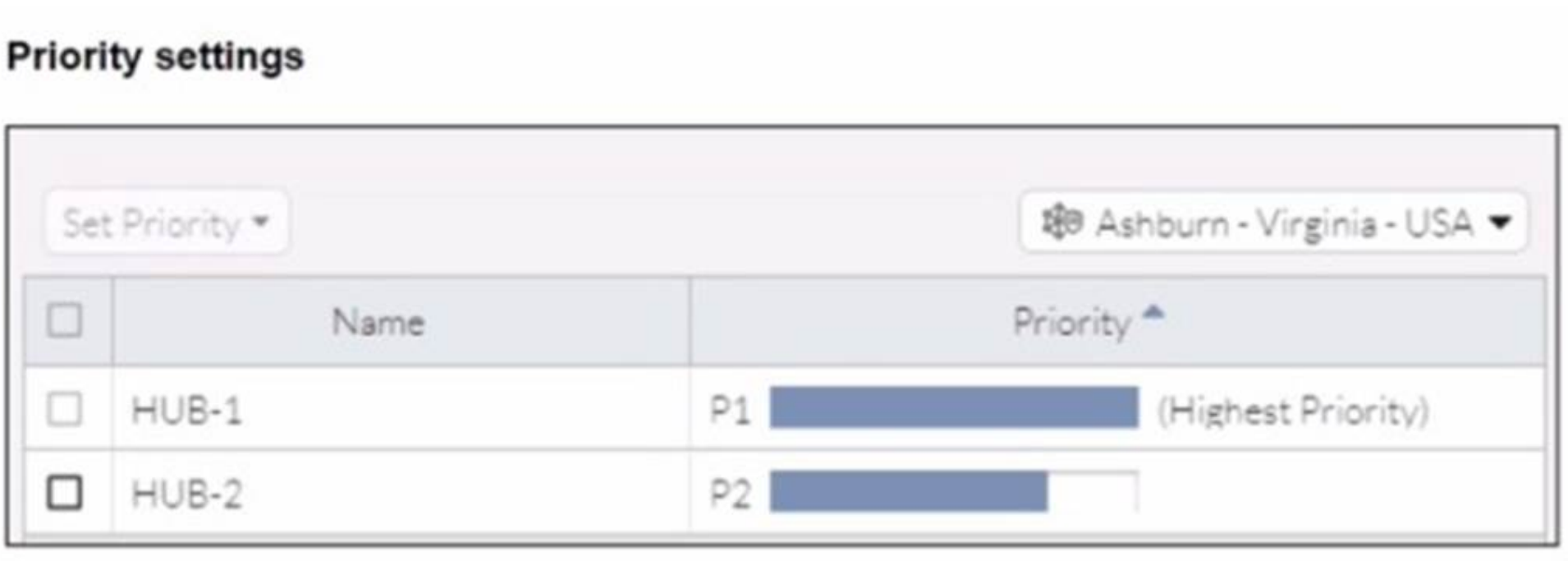
A. intrusion prevention system (IPS)
B. SSL deep inspection
C. DNS filter
D. Web filter with inline-CASB

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 6
Refer to the exhibits.





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: C

Explanation:
When remote users connected to FortiSASE require access to internal resources on Branch-2, the following process occurs:
? SD-WAN Capability:
? Traffic Routing Decision:
? Branch-2 Access:
References:
? FortiOS 7.2 Administration Guide: Details on SD-WAN configurations and priority settings.
? FortiSASE 23.2 Documentation: Explains how FortiSASE integrates with SD-WAN to route traffic based on defined priorities and performance metrics.

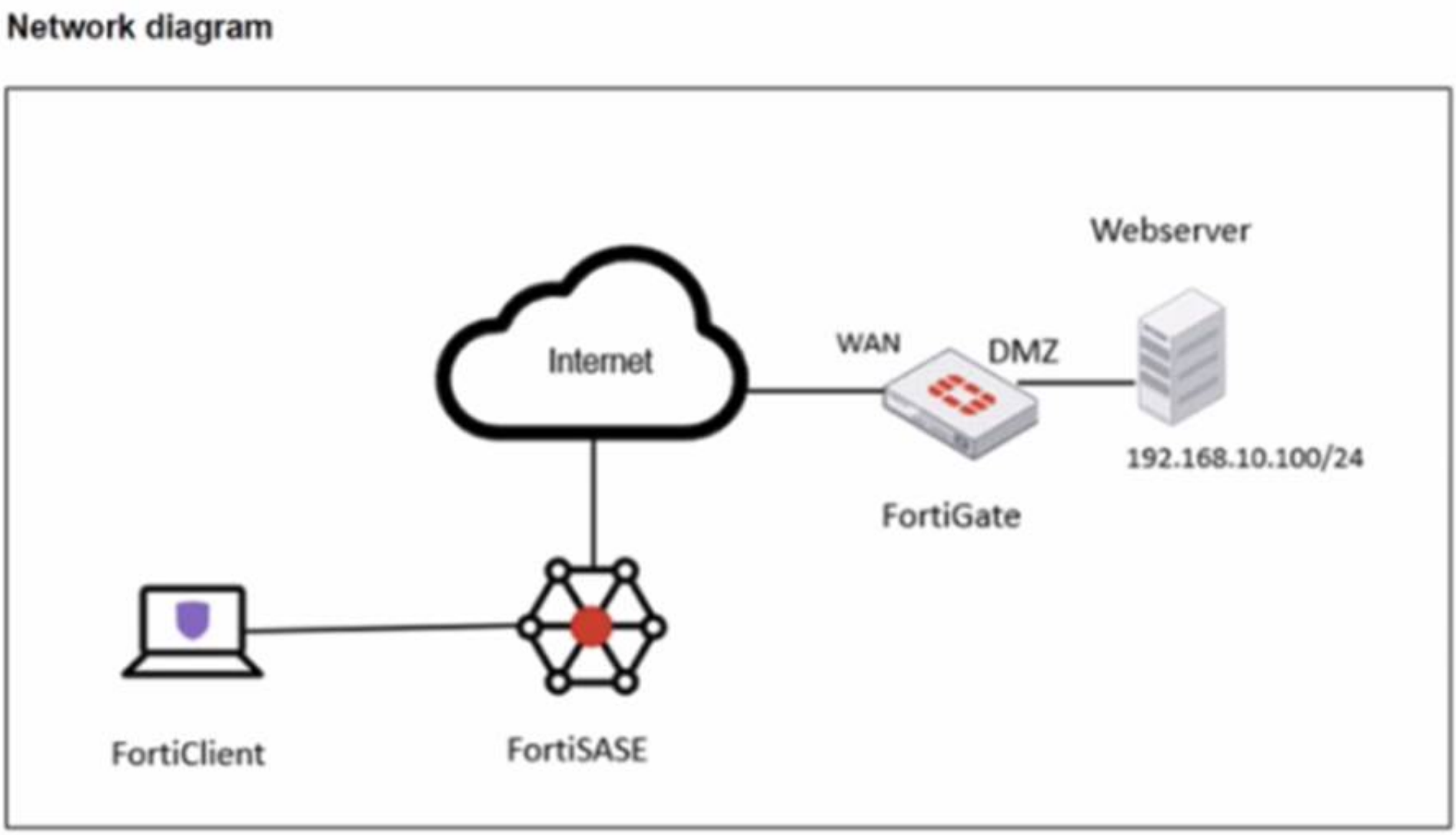
NEW QUESTION 7
A FortiSASE administrator is configuring a Secure Private Access (SPA) solution to share endpoint information with a corporate FortiGate.
Which three configuration actions will achieve this solution? (Choose three.)

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 8
Refer to the exhibits.

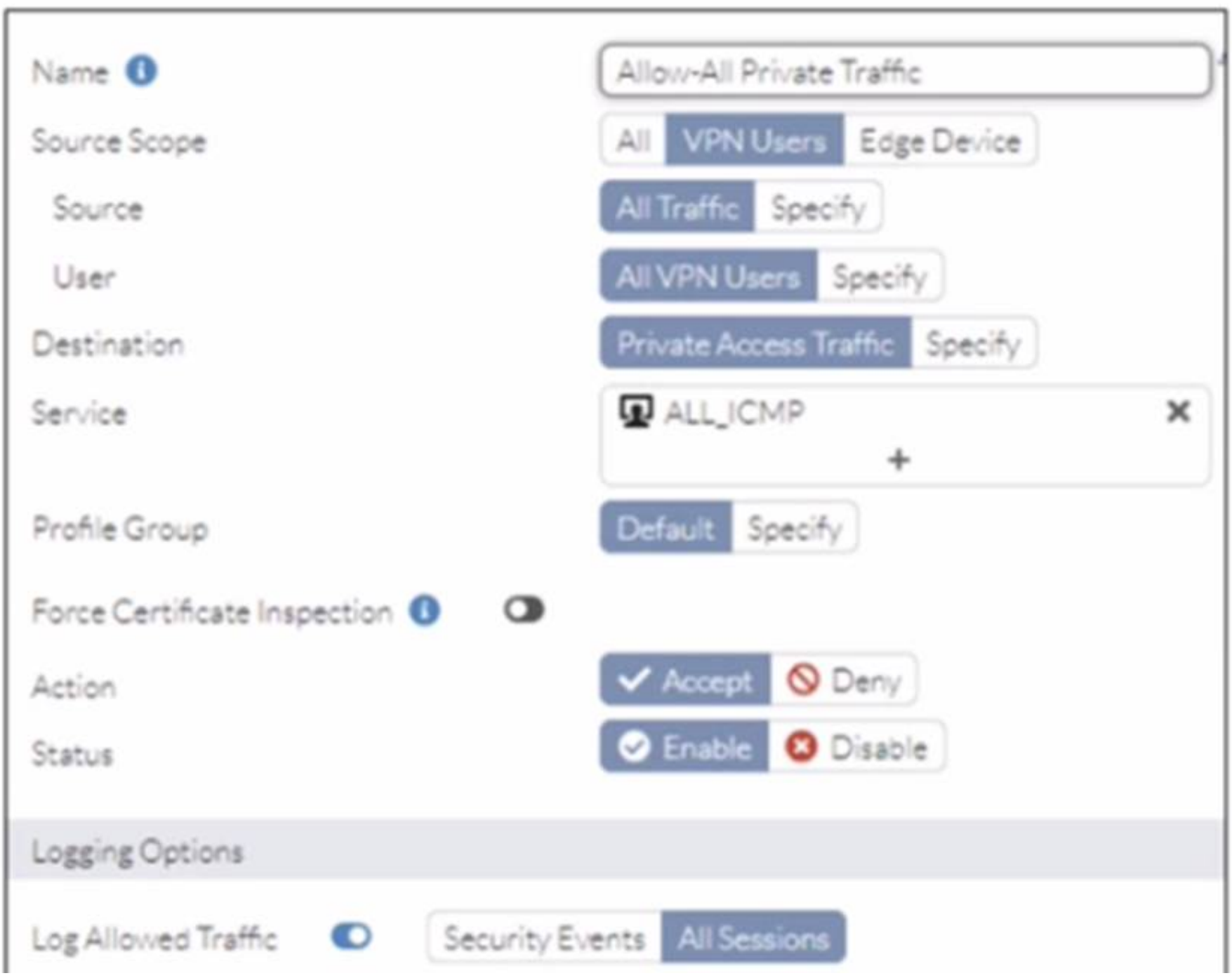


VPN tunnel diagnose output on FortiGate Hub

```
# 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 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



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 FortiGale 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 9
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 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
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCSS_SASE_AD-23 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCSS_SASE_AD-23 Product From:

https://www.2passeasy.com/dumps/FCSS_SASE_AD-23/

Money Back Guarantee

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