# Free Questions for FCSS_SASE_AD-23 by certsinside

## Shared by Marshall on 26-06-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

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.)

## Options:

**A-** SSL deep inspection

**B-** Split DNS rules

**C-** Split tunnelling destinations

**D-** DNS filter

## Answer:

B, C

## 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 DNS allows the configuration of specific DNS queries to be directed to internal DNS servers instead of public DNS servers.

This ensures that internal hostnames are resolved using the organization's internal DNS infrastructure, maintaining privacy and accuracy for internal network resources.

Split Tunneling Destinations:

Split tunneling allows specific traffic (such as DNS queries for internal domains) to be routed through the VPN tunnel while other traffic is sent directly to the internet.

By configuring split tunneling destinations, you can ensure that DNS queries for internal hostnames are directed through the VPN to the internal DNS servers.

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.

# Question 2

**Question Type:** **MultipleChoice**

During FortiSASE provisioning, how many security points of presence (POPs) need to be configured by the FortiSASE administrator?

## Options:

**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):

A PoP is a strategically located data center that provides security services such as secure web gateway, firewall, and VPN termination.

Configuring at least one PoP ensures that users can connect to FortiSASE and benefit from its security features.

Scalability:

While only one PoP is required to start, additional PoPs can be added as needed to enhance redundancy, load balancing, and performance.

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.

# Question 3

**Question Type:** MultipleChoice

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

## Options:

**A-** Endpoint management

**B-** Points of presence

**C-** SD-WAN hub

**D-** Logging

**E-** Authentication

## Answer:

A, B, D

## Explanation:

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

Endpoint Management:

The data center location for endpoint management ensures that endpoint data and policies are managed and stored within the chosen geographical region.

Points of Presence (PoPs):

Points of Presence (PoPs) are the locations where FortiSASE services are delivered to users. Selecting PoP locations ensures optimal performance and connectivity for users based on their geographical distribution.

Logging:

The data center location for logging determines where log data is stored and managed. This is crucial for compliance and regulatory requirements, as well as for efficient log analysis and reporting.

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.

# Question 4

**Question Type:** MultipleChoice

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

## Options:

**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 each branch.

## Answer:

A, D

## Explanation:

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

Centralized Management for Simplified Administration:

FortiSASE provides a centralized management platform that allows administrators to manage security policies, configurations, and monitoring from a single interface.

This simplifies the administration and reduces the complexity of managing multiple branch offices.

Eliminates the Need for On-Premises Firewalls:

FortiSASE enables secure access to the internet and cloud applications without requiring dedicated on-premises firewalls at each branch office.

This reduces hardware costs and simplifies network architecture, as security functions are handled by the cloud-based FortiSASE solution.

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.

# Question 5

**Question Type:** MultipleChoice

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

## Options:

**A-** intrusion prevention system (IPS)

**B-** SSL deep inspection

**C-** DNS filter

**D-** Web filter with inline-CASB

## Answer:

B, D

## Explanation:

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

SSL Deep Inspection:

SSL deep inspection is essential for decrypting and inspecting HTTPS traffic to identify and control applications and data transfers within encrypted traffic.

This allows FortiSASE to enforce security policies on SSL/TLS encrypted traffic, providing visibility and control over cloud applications.

Web Filter with Inline-CASB:

The web filter component integrates with inline-CASB to monitor and control access to cloud applications based on predefined security policies.

This combination provides granular control over cloud application usage, ensuring compliance with security policies and preventing unauthorized data transfers.

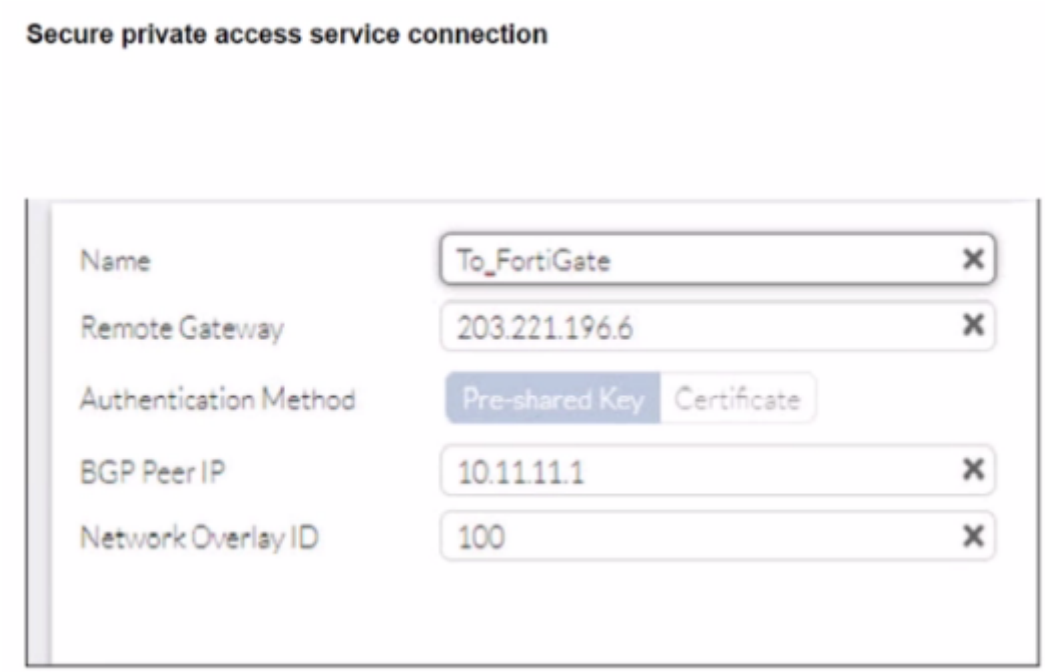
FortiOS 7.2 Administration Guide: Details on SSL deep inspection and web filtering configurations.

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

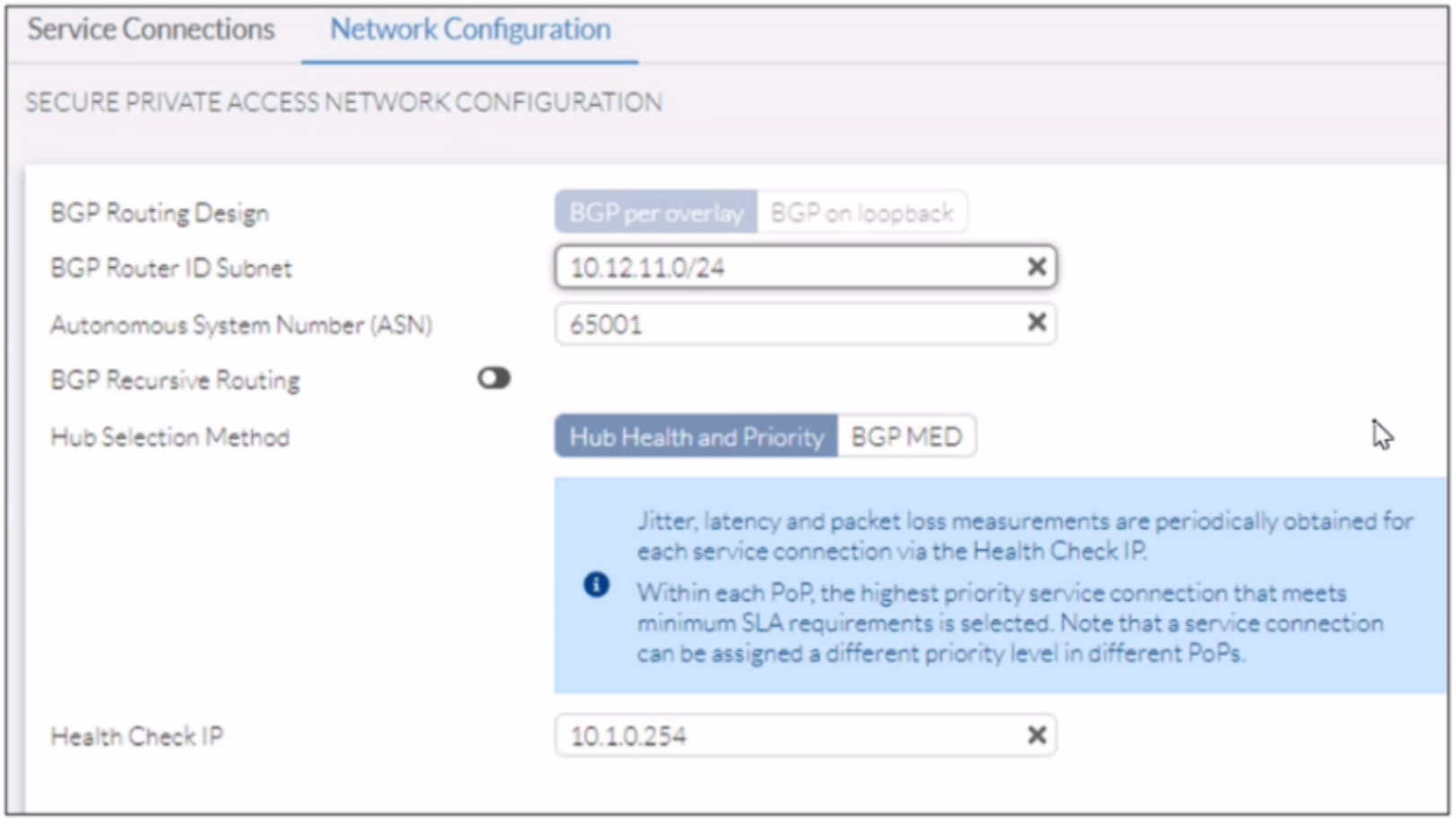
# Question 6

**Question Type:** **MultipleChoice**

Refer to the exhibits.



**Secure private access network connection**



**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 SblOigpvIFFYSpRZ/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?

## Options:

**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:

C

## Explanation:

The VPN tunnel between the FortiSASE spoke and the FortiGate hub is not establishing due to the configuration of mode config, which is not supported by FortiSASE spoke devices. Mode config is used to assign IP addresses to VPN clients dynamically, but this feature is not applicable to FortiSASE spokes.

Mode Config in IPsec:

The configuration snippet shows that mode config is enabled in the IPsec phase 1 settings.

Mode config is typically used for VPN clients to dynamically receive an IP address from the VPN server, but it is not suitable for site-to-site VPN configurations involving FortiSASE spokes.

Configuration Adjustment:

To establish the VPN tunnel, you need to disable mode config in the IPsec phase 1 settings.

This adjustment will allow the FortiSASE spoke to properly establish the VPN tunnel with the FortiGate hub.

Steps to Disable Mode Config:

Access the VPN configuration on the FortiSASE spoke.

Edit the IPsec phase 1 settings to disable mode config.

Ensure other settings such as pre-shared key, remote gateway, and BGP configurations are correct and consistent with the FortiGate hub.

FortiOS 7.2 Administration Guide: Provides details on configuring IPsec VPNs and mode config settings.

FortiSASE 23.2 Documentation: Explains the supported configurations for FortiSASE spoke devices and VPN setups.

## Question 7

**Question Type:** MultipleChoice

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 end points?

## Options:

**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:

Agentless deployment allows remote users to connect to the SIA service without needing to install any client software or configure browser settings.

This approach reduces the setup and maintenance overhead for both users and administrators.

Minimized Setup:

Without the need for FortiClient installation or explicit proxy configuration, the deployment is straightforward and quick.

Users can securely access the internet with minimal disruption and administrative effort.

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.

# Question 8

**Question Type:** **MultipleChoice**

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?

## Options:

**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):

ZTNA operates on the principle of 'never trust, always verify,' continuously verifying user identity and device security posture before granting access.

It provides secure and granular access to specific applications, ensuring that remote users can securely access the TCP-based application hosted on the private web server.

Secure and Efficient Access:

ZTNA private access allows remote users to connect directly to the application without needing a full VPN tunnel, reducing latency and improving performance.

It ensures that only authorized users can access the application, providing robust security controls.

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

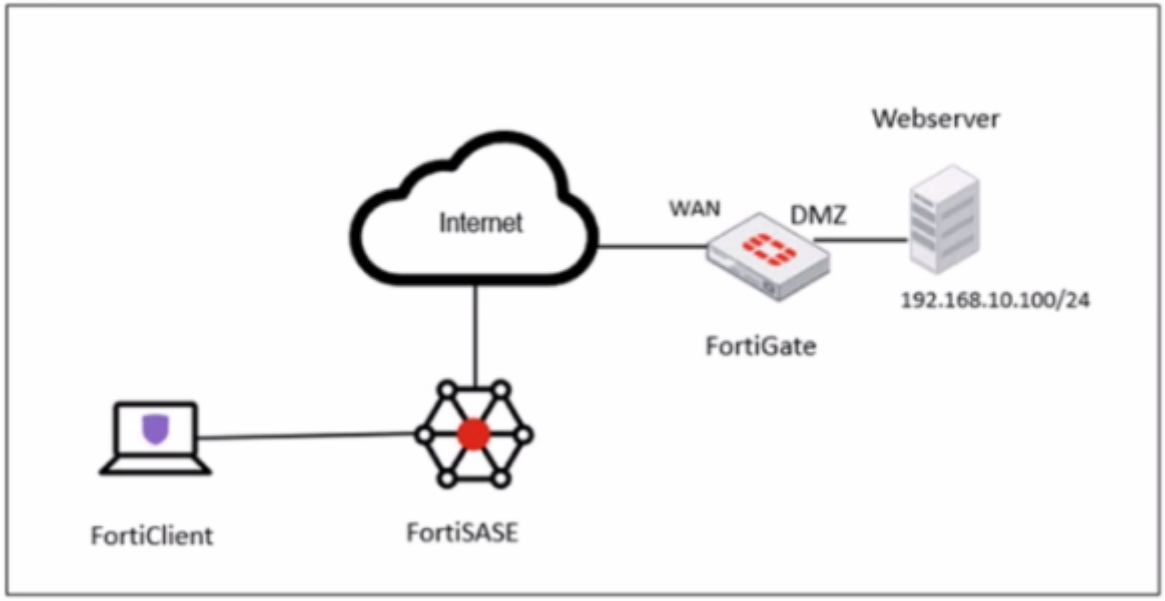
FortiSASE 23.2 Documentation: Explains how ZTNA can be used to provide secure access to private applications for remote users.

# Question 9

**Question Type:** **MultipleChoice**

Refer to the exhibits.

**Network diagram**

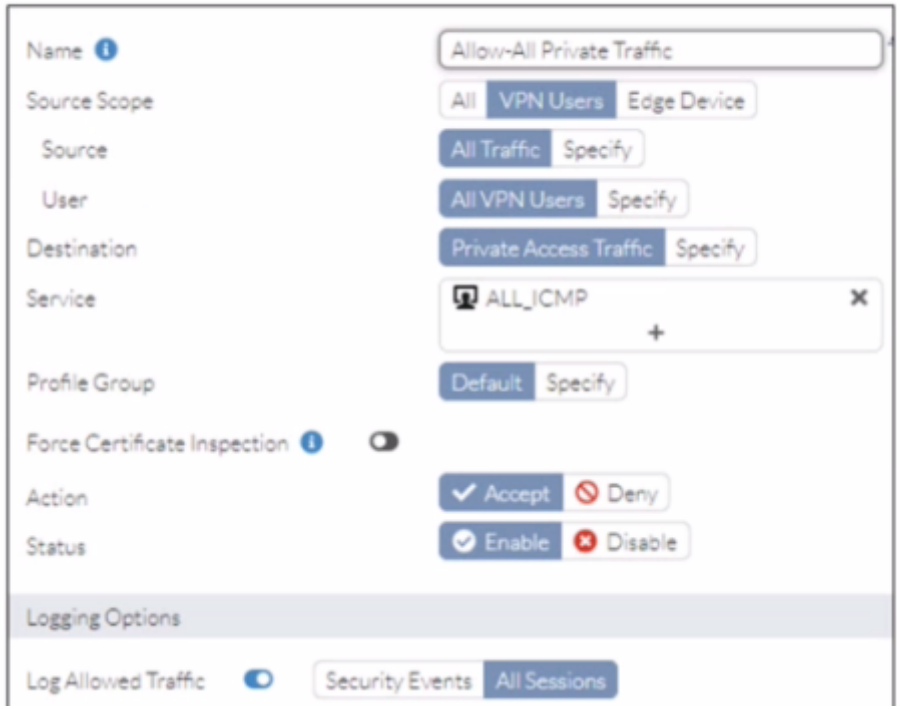


### VPN tunnel diagnose output on FortiGate Hub

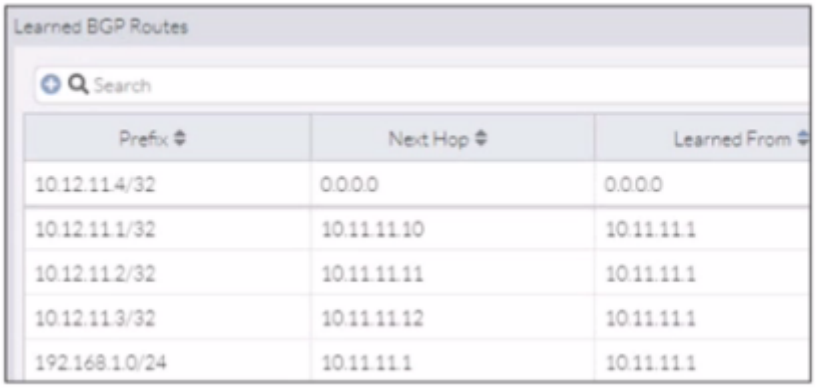
```
# diagnose vpn tunnel list name SASE_0
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=SASE_0 ver=2 serial=14 172.16.10.101:4500->172.16.10.1:64916 tun_id=10.11.11.10 tun_id6=::10.0.0.18 dst_mtu=150
bound_if=6 lgwy=static/1 tun=intf mode=dial_inst/3 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**



**BGP route information on FortiSASE**



**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?

## Options:

**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:

Quick mode selectors specify the source and destination subnets that are allowed to communicate through the VPN tunnel.

If the selectors do not include the subnet of the webserver (192.168.10.0/24), then the traffic will be restricted, and the ping will fail.

Diagnostic Output:

The diagnostic output shows the VPN configuration details, but it is important to check the quick mode selectors to ensure that the necessary subnets are included.

If the quick mode selectors are too restrictive, they will prevent traffic to and from the specified subnets.

Configuration Check:

Verify the quick mode selectors on both the FortiSASE and FortiGate hub to ensure they match and include the subnet of the webserver.

Adjust the selectors to allow the necessary subnets for successful communication.

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.

# Question 10

**Question Type:** **MultipleChoice**

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?

## Options:

**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:

FortiClient is a comprehensive endpoint security solution that integrates with FortiSASE to provide continuous protection for remote user endpoints.

It ensures that endpoints are always connected to the FortiSASE infrastructure, even when users are off the corporate network.

Always-On Security:

The unified FortiClient maintains a persistent connection to FortiSASE, enforcing security policies and protecting endpoints against threats at all times.

This ensures compliance with the cybersecurity policy requiring constant connectivity and protection for remote users.

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.

# Question 11

**Question Type:** MultipleChoice

When viewing the daily summary report generated by FortiSASE. the administrator notices that the report contains very little dat

a. What is a possible explanation for this almost empty report?

## Options:

**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:

The 'Log allowed traffic' setting determines which types of traffic are logged.

When set to 'Security Events,' only traffic that triggers a security event (such as a threat detection or policy violation) is logged.

Impact on Report Data:

If the log setting excludes regular allowed traffic, the amount of data captured and reported is significantly reduced.

This results in reports with minimal data, as only security-related events are included.

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.