Fortinet.FCSS_SASE_AD-24.by.Sodu.22q

Number: FCSS_SASE_AD-24
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: FCSS_SASE_AD-24

Exam Name: FCSS - FortiSASE 24 Administrator

Exam A

QUESTION 1

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

Correct Answer: B
Section:

QUESTION 2

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

Correct Answer: A, B
Section:
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 3

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?

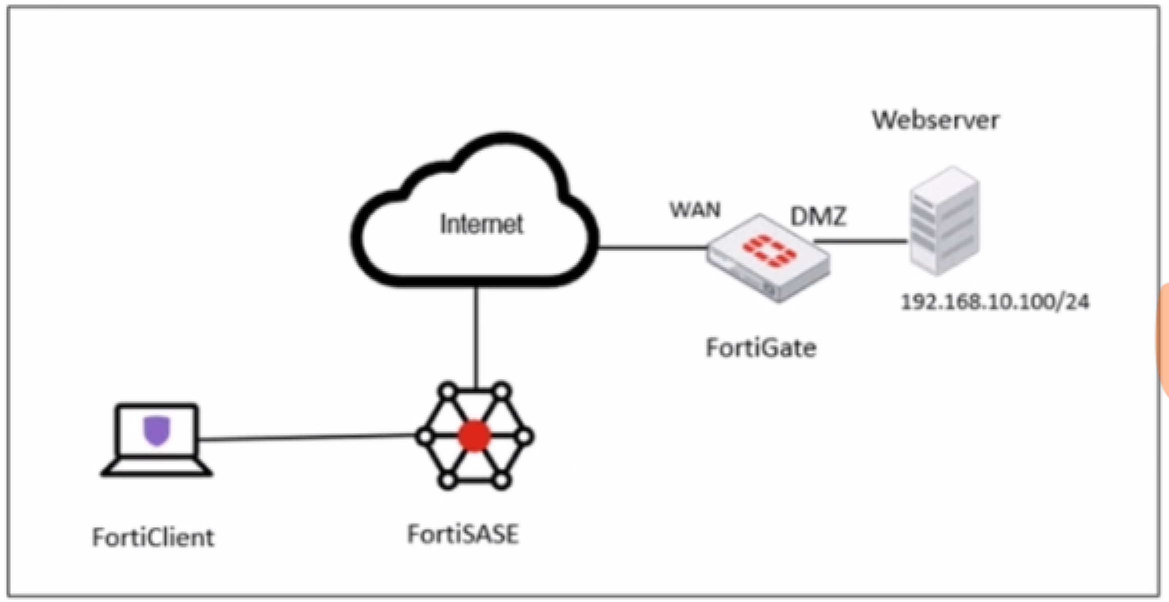
A. site-based deployment
B. thin-branch SASE extension
C. unified FortiClient
D. inline-CASB

Correct Answer: C

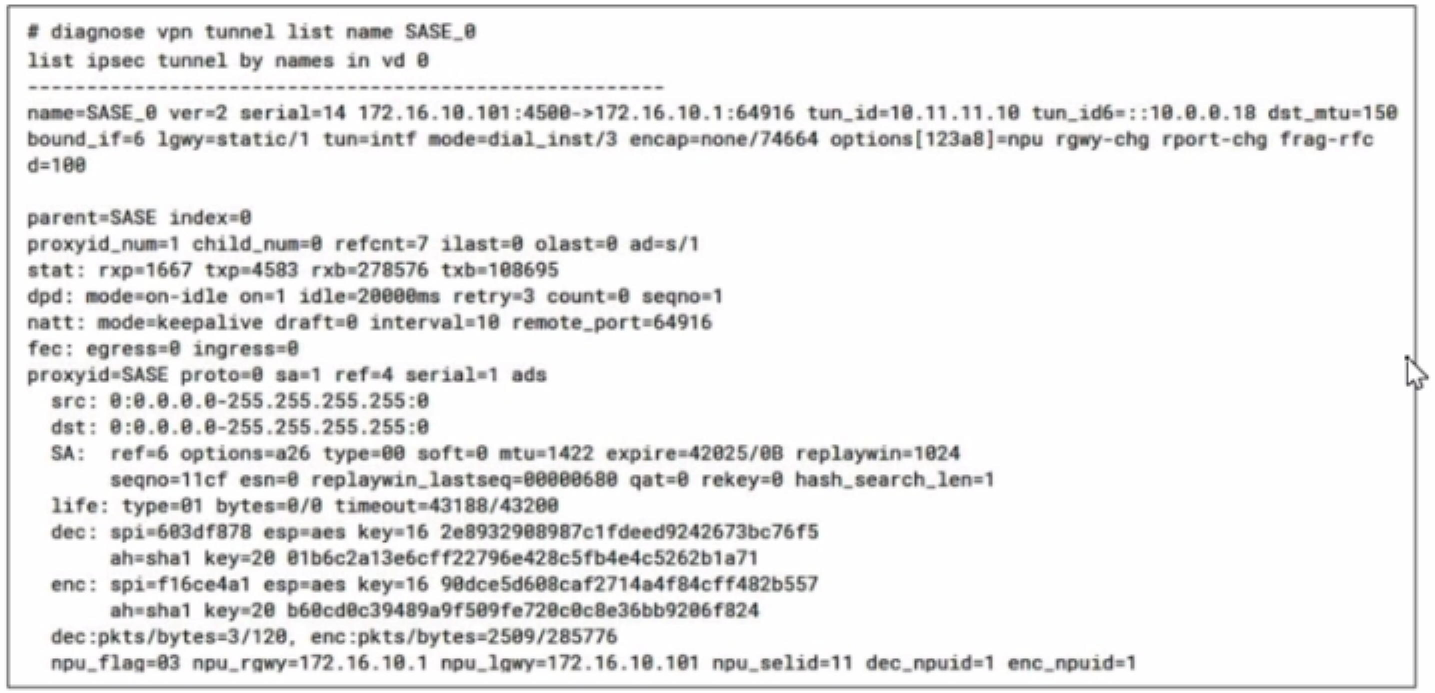
Section:
Explanation:
The unified FortiClient component of FortiSASE facilitates the always-on security measure required for ensuring that all remote user endpoints are always connected and protected.
Unified FortiClient:
FortiClient is a comprehensive endpoint security solution that integrates with 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 4
Refer to the exhibits.

Network diagram



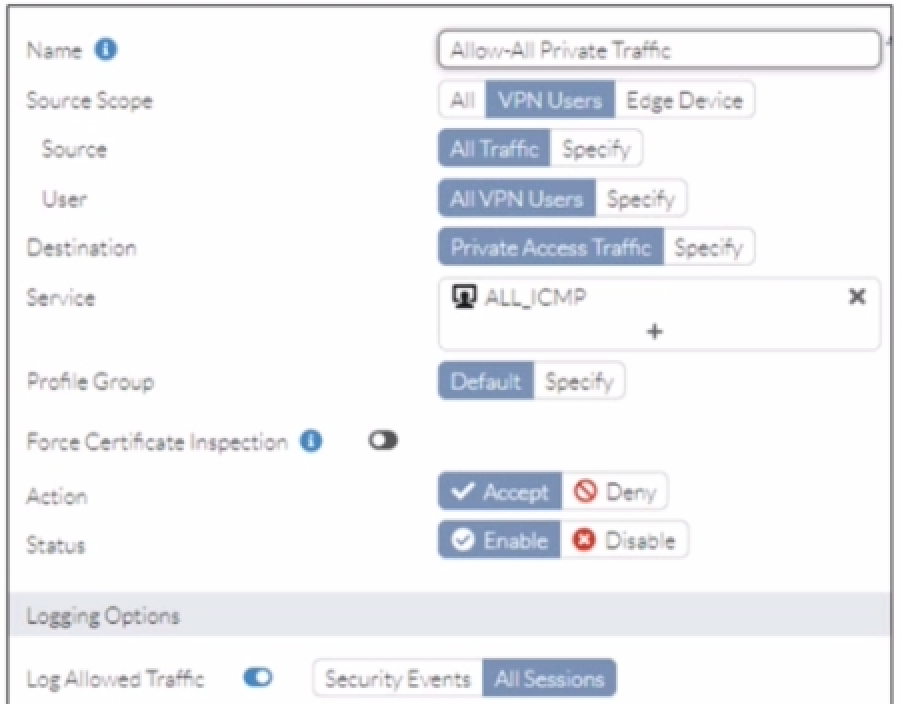
VPN tunnel diagnose output on FortiGate Hub



```
# 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
```

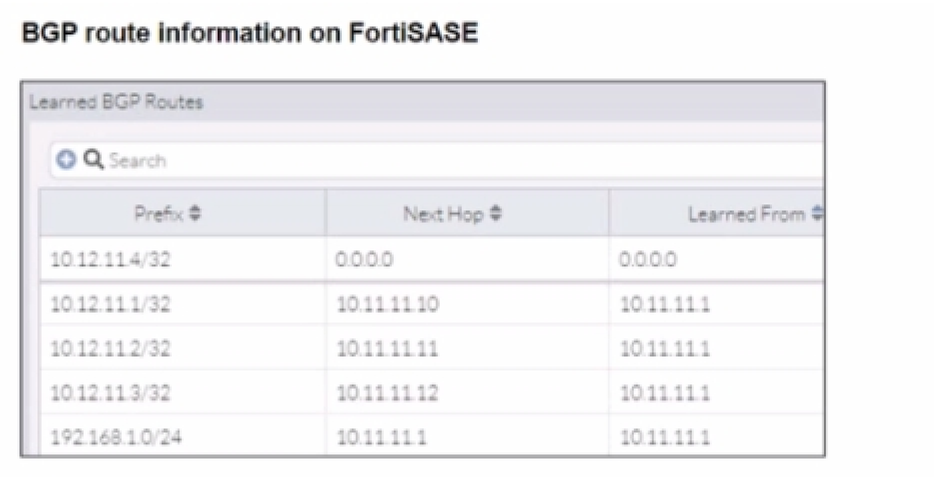
Secure Private Access policy on FortiSASE



Name	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

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

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.

Correct Answer: C
Section:

QUESTION 5
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)

Correct Answer: C
Section:
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.

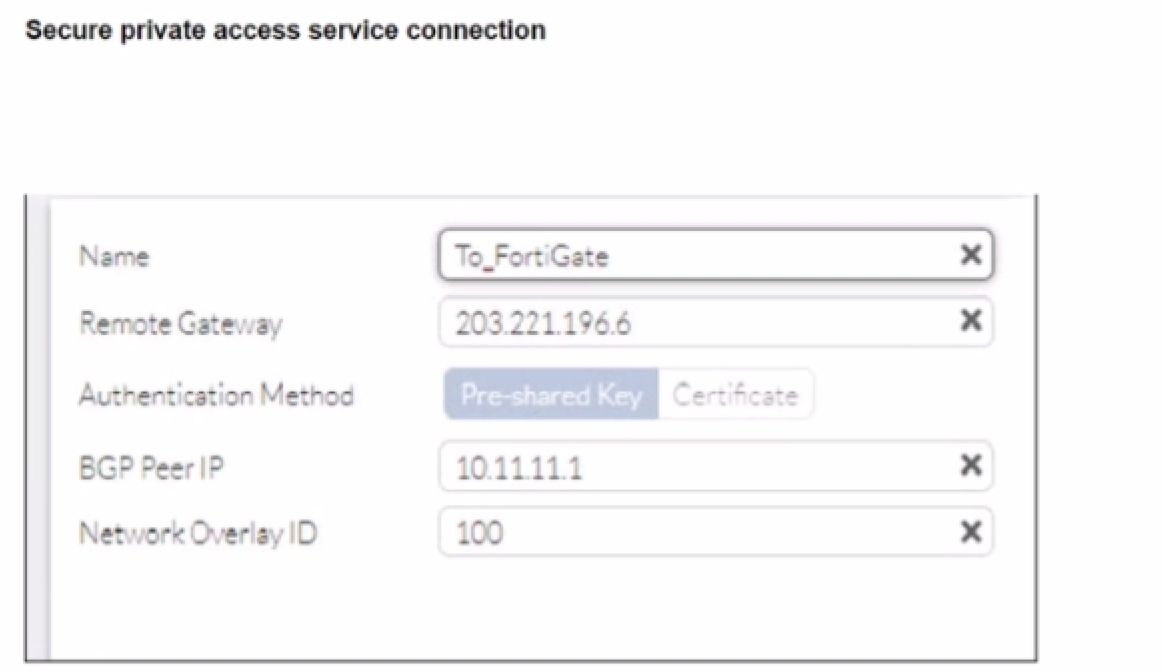
QUESTION 6
Which secure internet access (SIA) use case minimizes individual workstation or device setup, because you do not need to install FortiClient on endpoints or configure explicit web proxy settings on web browser-based end

points?

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

Correct Answer: B
Section:
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.

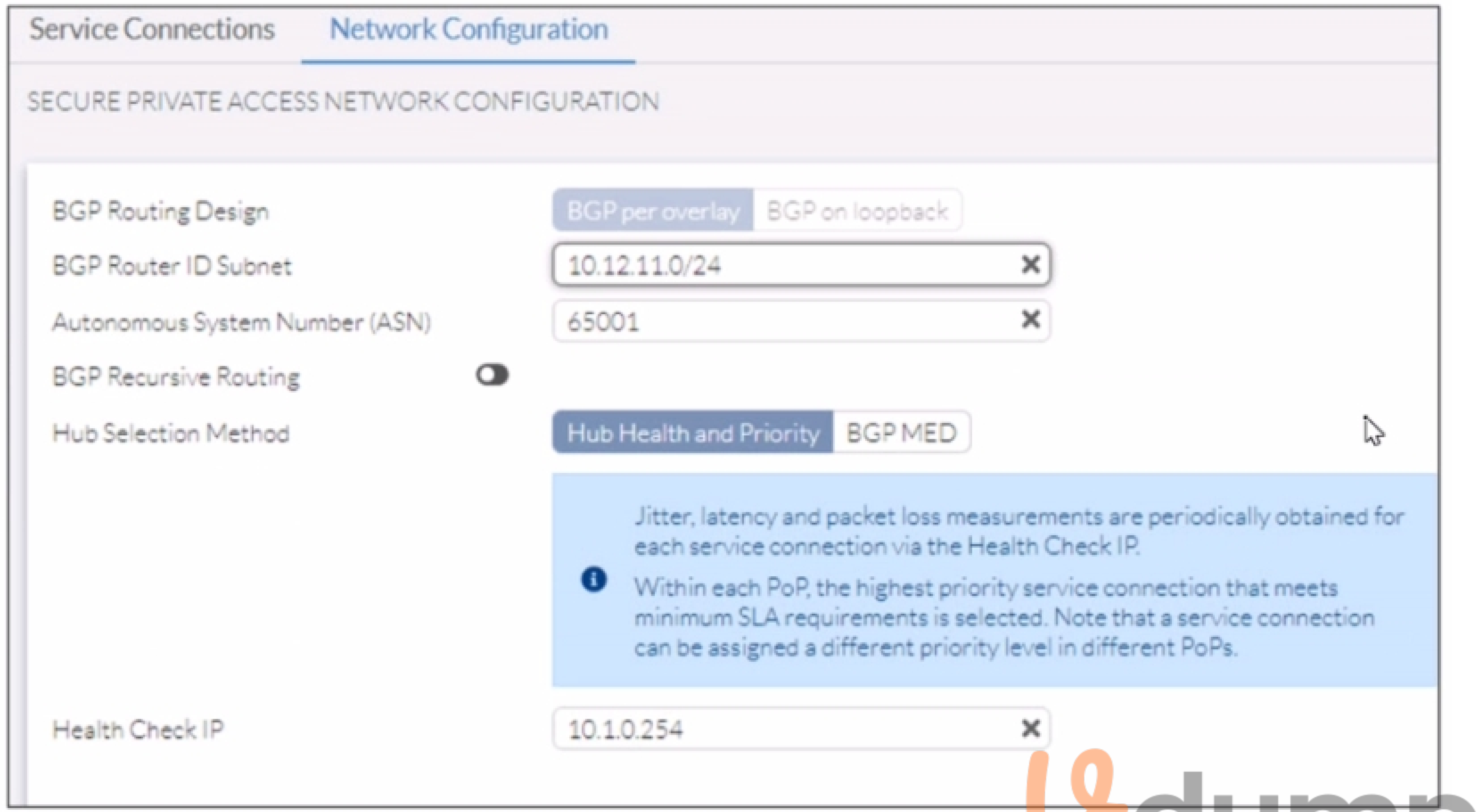
QUESTION 7
Refer to the exhibits.



Secure private access service connection

Name	To_FortiGate
Remote Gateway	203.221.196.6
Authentication Method	Pre-shared Key / Certificate
BGP Peer IP	10.11.11.1
Network Overlay ID	100

Secure private access network connection



SECURE PRIVATE ACCESS NETWORK CONFIGURATION

BGP Routing Design: BGP per overlay | BGP on loopback

BGP Router ID Subnet: 10.12.11.0/24

Autonomous System Number (ASN): 65001

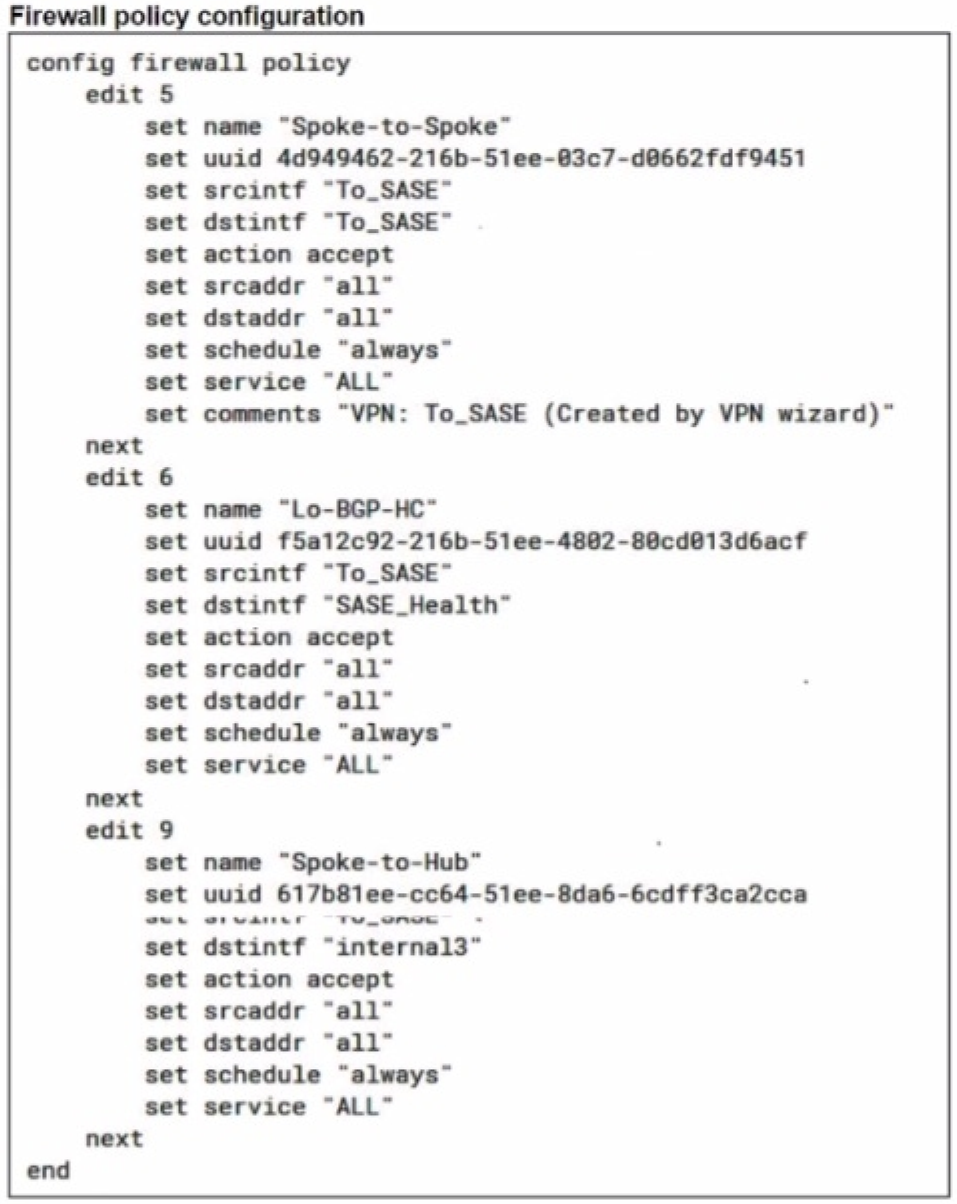
BGP Recursive Routing

Hub Selection Method: Hub Health and Priority | BGP MED

Jitter, latency and packet loss measurements are periodically obtained for each service connection via the Health Check IP.

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.

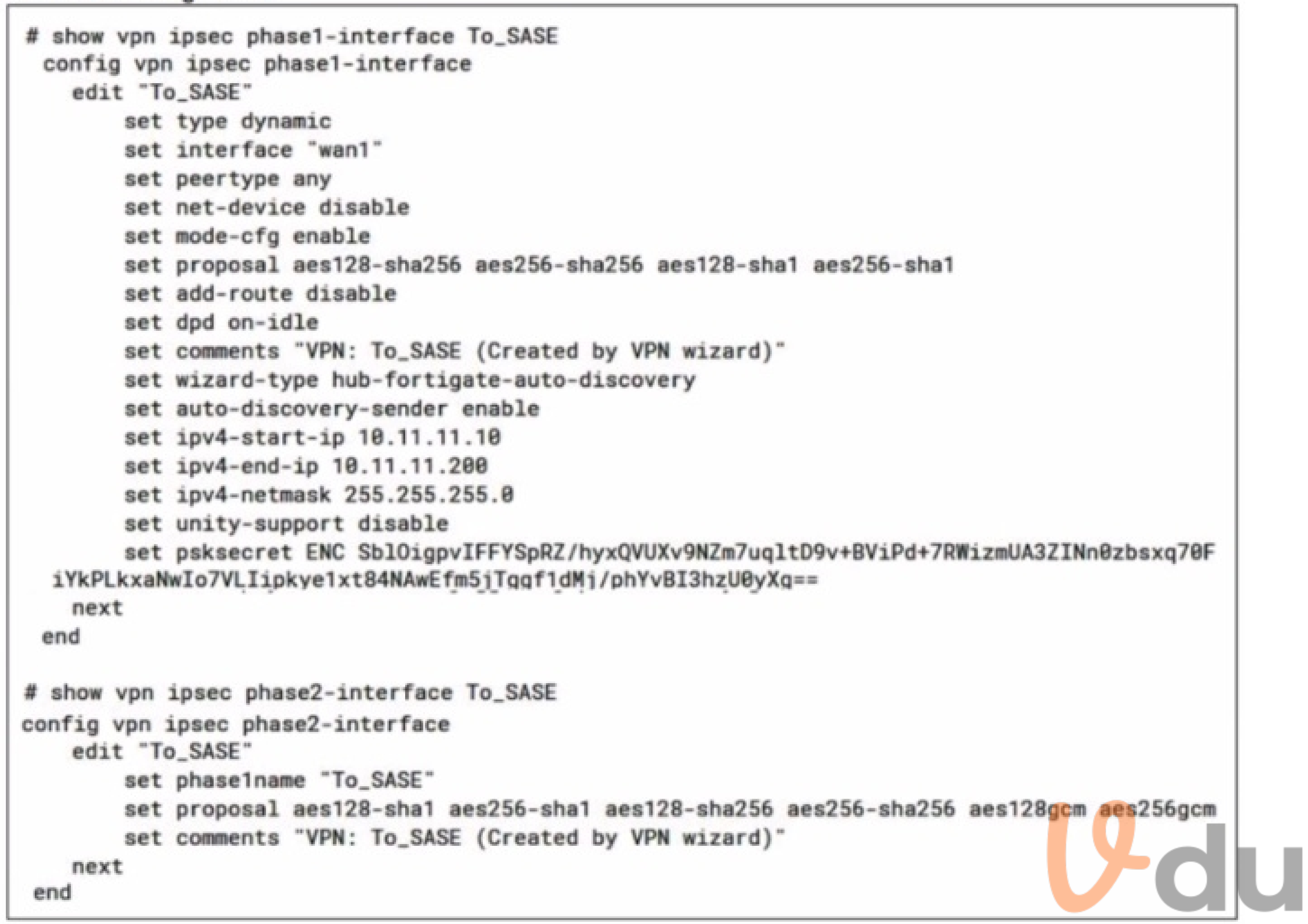
Health Check IP: 10.1.0.254



Firewall policy configuration

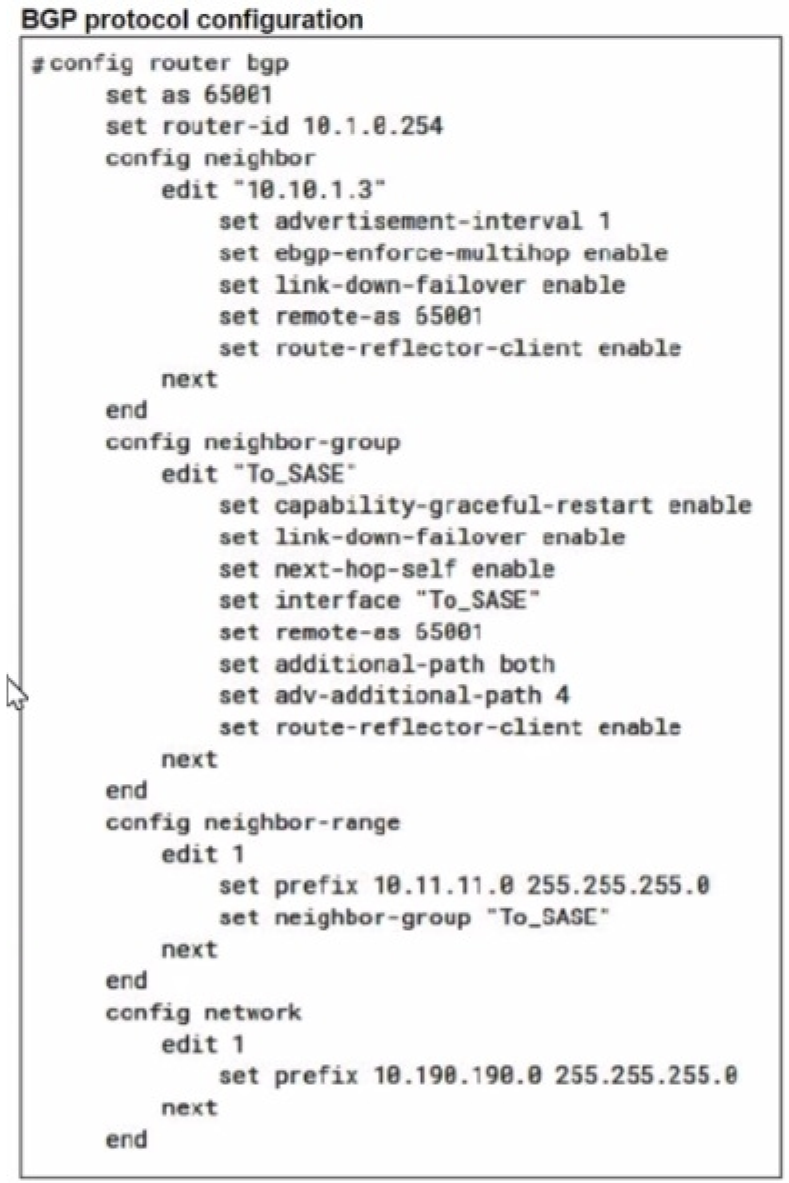
```
config firewall policy
    edit 5
        set name "Spoke-to-Spoke"
        set uuid 4d949462-216b-51ee-03c7-d0662fdf9451
        set srcintf "To_SASE"
        set dstintf "To_SASE"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        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?

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.

Correct Answer: D
Section:

QUESTION 8
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

Correct Answer: A, B
Section:

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 each branch.

Correct Answer: A, D
Section:
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 10
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

Correct Answer: A, B, D
Section:
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 11
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. Log allowed traffic is set to Security Events for all policies.
B. There are no security profile groups applied to all policies.
C. The web filter security profile is not set to Monitor.
D. Digital experience monitoring is not configured.

Correct Answer: A
Section:
Explanation:
The issue of an almost empty daily summary report in FortiSASE can often be traced back to how logging is configured within the system. Specifically, if 'Log Allowed Traffic' is set to 'Security Events' for all policies, it means that only security-related events (such as threats or anomalies) are being logged, while normal, allowed traffic is not being recorded. Since most traffic in a typical network environment is allowed, this configuration would result in very little data being captured and subsequently reported in the daily summary.
Here's a breakdown of why the other options are less likely to be the cause:
B . There are no security profile groups applied to all policies: While applying security profiles is important for comprehensive protection, their absence does not directly affect the volume of data in reports unless specific logging settings are also misconfigured.
C . The web filter security profile is not set to Monitor: This option pertains specifically to web filtering activities. Even if web filtering is not set to monitor mode, other types of traffic and logs should still populate the report.
D . Digital experience monitoring is not configured: Digital Experience Monitoring (DEM) focuses on user experience metrics rather than general traffic logging. Its absence would not lead to an almost empty report.
To resolve this issue, administrators should review the logging settings across all policies and ensure that 'Log Allowed Traffic' is appropriately configured to capture the necessary data for reporting purposes.
Fortinet FCSS FortiSASE Documentation - Reporting and Logging Best Practices
FortiSASE Administration Guide - Configuring Logging Settings

QUESTION 12
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

Correct Answer: A, B
Section:
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:
The FortiSASE CA certificate is essential for establishing trust between the endpoint and the FortiSASE infrastructure.
It ensures that the endpoint can securely communicate with FortiSASE services and inspect SSL/TLS traffic.
Proxy Auto-Configuration (PAC) File:
The PAC file is used to configure the endpoint to direct web traffic through the FortiSASE proxy.
It provides instructions on how to route traffic, ensuring that all web requests are properly inspected and filtered by FortiSASE.
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.

QUESTION 13
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.

Correct Answer: A, C
Section:
Explanation:
There are two deployment methods used to connect a FortiExtender as a FortiSASE LAN extension:
Connect FortiExtender to FortiSASE using FortiZTP:
FortiZero Touch Provisioning (FortiZTP) simplifies the deployment process by allowing FortiExtender to automatically connect and configure itself with FortiSASE.
This method requires minimal manual configuration, making it efficient for large-scale deployments.
Enter the FortiSASE domain name in the FortiExtender GUI as a static discovery server:
Manually configuring the FortiSASE domain name in the FortiExtender GUI allows the extender to discover and connect to the FortiSASE infrastructure.
This static discovery method ensures that FortiExtender can establish a connection with FortiSASE using the provided domain name.
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.

QUESTION 14

Your organization is currently using FortiSASE for its cybersecurity. They have recently hired a contractor who will work from the HQ office and who needs temporary internet access in order to set up a web-based point of sale (POS) system.
What is the recommended way to provide internet access to the contractor?

A. Use FortiClient on the endpoint to manage internet access.

B. Use a proxy auto-configuration (PAC) file and provide secure web gateway (SWG) service as an explicit web proxy.

C. Use zero trust network access (ZTNA) and tag the client as an unmanaged endpoint.

D. Configure a VPN policy on FortiSASE to provide access to the internet.

Correct Answer: C
Section:
Explanation:
The recommended way to provide temporary internet access to the contractor is to use Zero Trust Network Access (ZTNA) and tag the client as an unmanaged endpoint . ZTNA ensures that only authorized users and devices can access specific resources, while treating all endpoints as untrusted by default. By tagging the contractor's device as an unmanaged endpoint, you can apply strict access controls and ensure that the contractor has limited access to only the necessary resources (e.g., the web-based POS system) without exposing the internal network to unnecessary risks.
Here's why the other options are less suitable:
A . Use FortiClient on the endpoint to manage internet access: While FortiClient provides endpoint security and management, it requires installation and configuration on the contractor's device. This may not be feasible for temporary contractors or unmanaged devices.
B . Use a proxy auto-configuration (PAC) file and provide secure web gateway (SWG) service as an explicit web proxy: While this approach can control web traffic, it does not provide the granular access control and security posture validation offered by ZTNA. Additionally, managing PAC files can be cumbersome and less secure compared to ZTNA.
D . Configure a VPN policy on FortiSASE to provide access to the internet: Using a VPN policy would grant broader access to the network, which is not ideal for a temporary contractor. It increases the risk of unauthorized access to internal resources and does not align with the principle of least privilege.
Fortinet FCSS FortiSASE Documentation - Zero Trust Network Access (ZTNA) Use Cases
FortiSASE Administration Guide - Managing Unmanaged Endpoints

QUESTION 15

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.

Correct Answer: A, C
Section:
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.
Fortinet FCSS FortiSASE Documentation - ZTNA Private Access Overview
FortiSASE Administration Guide - ZTNA Deployment Best Practices

QUESTION 16
Which statement applies to a single sign-on (SSO) deployment on FortiSASE?

A. SSO overrides any other previously configured user authentication.

B. SSO identity providers can be integrated using public and private access types.

C. SSO is recommended only for agent-based deployments.

D. SSO users can be imported into FortiSASE and added to user groups.

Correct Answer: D
Section:
Explanation:
In a Single Sign-On (SSO) deployment on FortiSASE, SSO users can be imported into FortiSASE and added to user groups . This allows administrators to manage SSO users within FortiSASE, enabling them to apply policies, permissions, and group-based access controls. By integrating SSO with FortiSASE, organizations can streamline user authentication and simplify access management while maintaining security.
Here's why the other options are incorrect:
A . SSO overrides any other previously configured user authentication: This is incorrect because SSO does not automatically override other authentication methods. FortiSASE supports multiple authentication mechanisms, and SSO is just one of them. Administrators can configure fallback authentication methods if needed.
B . SSO identity providers can be integrated using public and private access types: While FortiSASE supports integration with various identity providers (e.g., SAML, LDAP, OAuth), the concept of 'public and private access types' is not applicable to SSO configurations.
C . SSO is recommended only for agent-based deployments: This is incorrect because SSO can be used in both agent-based and agentless deployments. It is not limited to environments where agents are installed.
Fortinet FCSS FortiSASE Documentation - Single Sign-On (SSO) Integration
FortiSASE Administration Guide - User Authentication and SSO

QUESTION 17
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.

Correct Answer: B
Section:
Explanation:
The FortiGuard forensics analysis feature on FortiSASE is designed to help customers identify 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.
Fortinet FCSS FortiSASE Documentation - FortiGuard Forensics Analysis
FortiSASE Administration Guide - Threat Detection and Response

QUESTION 18
A customer needs to implement device posture checks for their remote endpoints while accessing the protected server. They also want the TCP traffic between the remote endpoints and the protected servers to be processed by FortiGate.
In this scenario, which three setups will achieve the above requirements? (Choose three.)

A. Configure ZTNA tags on FortiGate.
B. Configure FortiGate as a zero trust network access (ZTNA) access proxy.
C. Configure ZTNA servers and ZTNA policies on FortiGate.
D. Configure private access policies on FortiSASE with ZTNA.
E. Sync ZTNA tags from FortiSASE to FortiGate.

Correct Answer: A, B, C
Section:
Explanation:
To meet the requirements of implementing device posture checks for remote endpoints and ensuring that TCP traffic between the endpoints and protected servers is processed by FortiGate, the following three setups are necessary:
Configure ZTNA tags on FortiGate (Option A):
ZTNA (Zero Trust Network Access) tags are used to define access control policies based on the security posture of devices. By configuring ZTNA tags on FortiGate, administrators can enforce granular access controls, ensuring that only compliant devices can access protected resources.
Configure FortiGate as a zero trust network access (ZTNA) access proxy (Option B):
FortiGate can act as a ZTNA access proxy, which allows it to mediate and secure connections between remote endpoints and protected servers. This setup ensures that all TCP traffic passes through FortiGate, enabling inspection and enforcement of security policies.
Configure ZTNA servers and ZTNA policies on FortiGate (Option C):
To enable ZTNA functionality, administrators must define ZTNA servers (the protected resources) and create ZTNA policies on FortiGate. These policies determine how traffic is routed, inspected, and controlled based on device posture and user identity.
Here's why the other options are incorrect:
D . Configure private access policies on FortiSASE with ZTNA: While FortiSASE supports ZTNA, the requirement specifies that TCP traffic must be processed by FortiGate. Configuring private access policies on FortiSASE would route traffic through FortiSASE instead of FortiGate, which does not meet the stated requirements.
E . Sync ZTNA tags from FortiSASE to FortiGate: Synchronizing ZTNA tags is unnecessary in this scenario because the focus is on FortiGate processing the traffic. The tags can be directly configured on FortiGate without involving FortiSASE.
Fortinet FCSS FortiSASE Documentation - Zero Trust Network Access (ZTNA) Deployment

FortiGate Administration Guide - ZTNA Configuration

QUESTION 19
Which of the following describes the FortiSASE inline-CASB component?

A. It provides visibility for unmanaged locations and devices.
B. It is placed directly in the traffic path between the endpoint and cloud applications.
C. It uses API to connect to the cloud applications.
D. It detects data at rest.

Correct Answer: B
Section:
Explanation:
The FortiSASE inline-CASB (Cloud Access Security Broker) component is designed to provide real-time security and visibility by being placed directly in the traffic path between the endpoint and cloud applications . Inline-CASB inspects traffic as it flows to and from cloud applications, enabling enforcement of security policies, detection of threats, and prevention of unauthorized access. This approach ensures that all interactions with cloud applications are monitored and controlled in real time.
Here's why the other options are incorrect:
A . It provides visibility for unmanaged locations and devices: While inline-CASB enhances visibility, its primary function is to inspect and secure traffic in real time. Visibility for unmanaged locations and devices is typically achieved through other components like endpoint agents or API-based CASB.
C . It uses API to connect to the cloud applications: API-based CASB is a different approach that relies on APIs provided by cloud applications to monitor and manage data. Inline-CASB operates directly in the traffic flow rather than using APIs.
D . It detects data at rest: Detecting data at rest is typically handled by Data Loss Prevention (DLP) tools or API-based CASB solutions. Inline-CASB focuses on inspecting traffic in motion, not data stored in cloud applications.
Fortinet FCSS FortiSASE Documentation - Inline-CASB Overview
FortiSASE Administration Guide - Cloud Application Security

QUESTION 20
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

Correct Answer: A
Section:
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.
Fortinet FCSS FortiSASE Documentation - Inline-CASB and Web Filtering
FortiSASE Administration Guide - Securing Cloud Applications

QUESTION 21
Which statement best describes the Digital Experience Monitor (DEM) feature on FortiSASE?

A. It provides end-to-end network visibility from all the FortiSASE security PoPs to a specific SaaS application.
B. It can be used to request a detailed analysis of the endpoint from the FortiGuard team.
C. It requires a separate DEM agent to be downloaded from the FortiSASE portal and installed on the endpoint.
D. It can help IT and security teams ensure consistent security monitoring for remote users.

Correct Answer: A
Section:
Explanation:
The Digital Experience Monitor (DEM) feature in FortiSASE is designed to provide end-to-end network visibility by monitoring the performance and health of connections between FortiSASE security Points of Presence (PoPs) and specific SaaS applications. This ensures that administrators can identify and troubleshoot issues related to latency, jitter, packet loss, and other network performance metrics that could impact user experience when accessing cloud-based services.
Here's why the other options are incorrect:
B . It can be used to request a detailed analysis of the endpoint from the FortiGuard team: This is incorrect because DEM focuses on network performance monitoring, not endpoint analysis. Endpoint analysis would typically involve tools like FortiClient or FortiEDR, not DEM.
C . It requires a separate DEM agent to be downloaded from the FortiSASE portal and installed on the endpoint: This is incorrect because DEM operates at the network level and does not require an additional agent to be installed on endpoints.
D . It can help IT and security teams ensure consistent security monitoring for remote users: While DEM indirectly supports security by ensuring optimal network performance, its primary purpose is to monitor and improve the digital experience rather than enforce security policies.
Fortinet FCSS FortiSASE Documentation - Digital Experience Monitoring Overview
FortiSASE Administration Guide - Configuring DEM

QUESTION 22
What are two requirements to enable the MSSP feature on FortiSASE? (Choose two.)

A. Add FortiCloud premium subscription on the root FortiCloud account.
B. Configure MSSP user accounts and permissions on the FortiSASE portal.
C. Assign role-based access control (RBAC) to IAM users using FortiCloud IAM portal.
D. Enable multi-tenancy on the FortiSASE portal.

Correct Answer: C, D
Section:
Explanation:
To enable the MSSP (Managed Security Service Provider) feature on FortiSASE, two key requirements must be met:
Assign role-based access control (RBAC) to IAM users using FortiCloud IAM portal (Option C):
RBAC is essential for managing permissions and ensuring that different customers (tenants) have appropriate access levels. The FortiCloud Identity and Access Management (IAM) portal allows administrators to define roles and assign them to users, ensuring secure and granular control over resources.
Enable multi-tenancy on the FortiSASE portal (Option D):
Multi-tenancy is a critical feature for MSSPs, as it allows them to manage multiple customer environments (tenants) from a single FortiSASE instance. Each tenant operates independently with its own configurations, policies, and reporting, while the MSSP retains centralized control.
Here's why the other options are incorrect:
A . Add FortiCloud premium subscription on the root FortiCloud account: While FortiCloud subscriptions may enhance functionality, they are not specifically required to enable the MSSP feature.
B . Configure MSSP user accounts and permissions on the FortiSASE portal: User accounts and permissions are managed through the FortiCloud IAM portal, not directly on the FortiSASE portal.
Fortinet FCSS FortiSASE Documentation - MSSP Feature Configuration
FortiSASE Administration Guide - Multi-Tenancy and RBAC Setup