ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

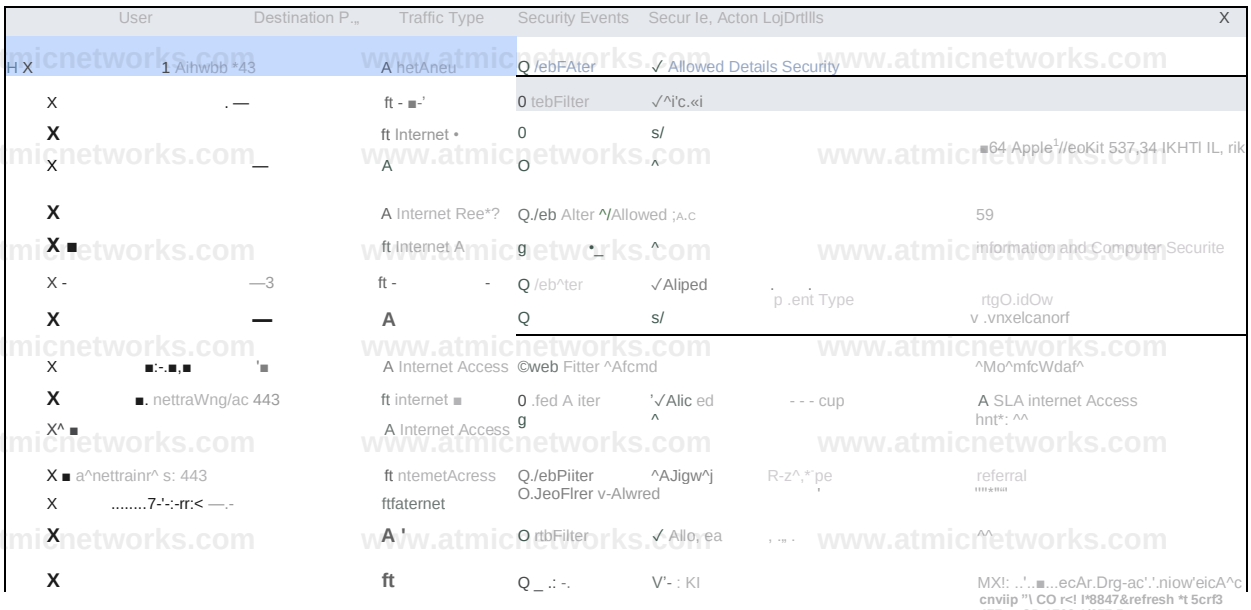
www.atmicnetworks .com

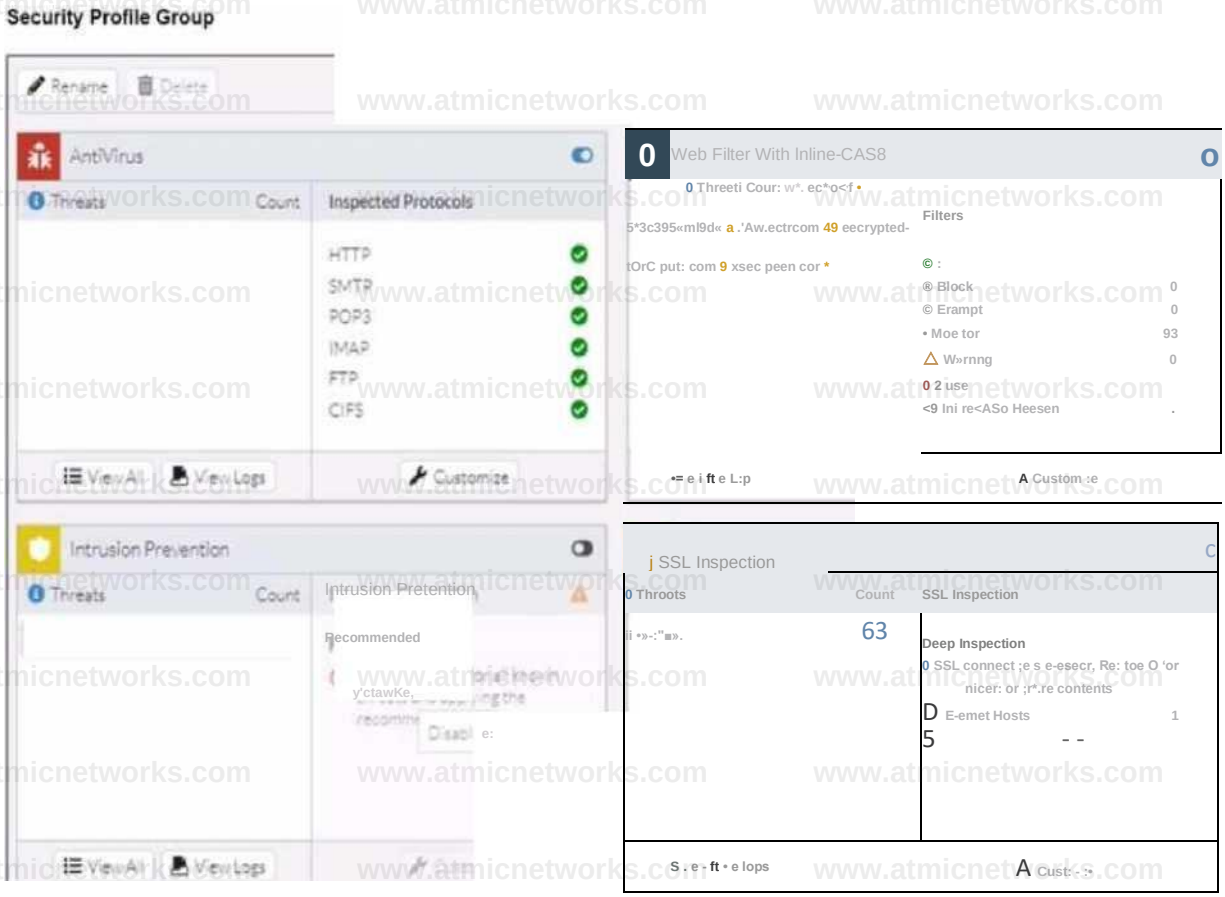
Warning: Keep connected with our support team for latest updates

Question: 1

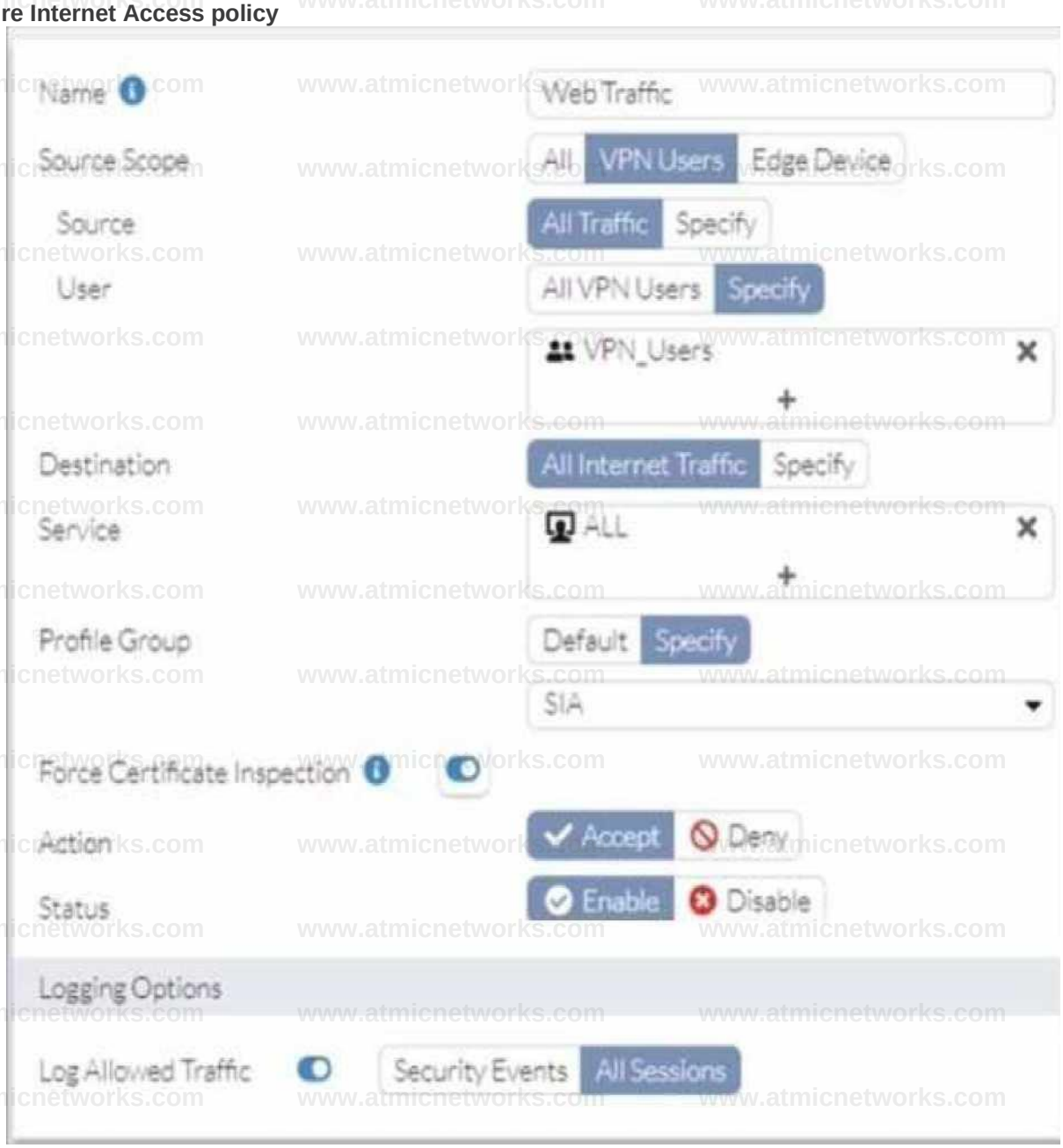
Refer to the exhibits.

Web Filtering logs





Secure Internet Access policy



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: D

Explanation:

The core of this issue lies in the difference between Certificate Inspection and Deep SSL Inspection within the FortiSASE security framework.

The Limitation of Certificate Inspection: When "Force Certificate Inspection" is enabled in a FortiSASE firewall policy, the system only inspects the SSL handshake—specifically the SNI (Server Name Indication) and certificate headers. It does not decrypt the actual data payload of the HTTPS session.

Antivirus Scanning Requirements: To detect and block malicious files like the EICAR test file when they are downloaded over an encrypted HTTPS connection (such as https://eicar.org), the FortiSASE antivirus engine must be able to "see" inside the encrypted tunnel. This requires Deep Inspection (Full SSL Inspection), where FortiSASE acts as a "man-in-the-middle" to decrypt, scan, and then reencrypt the traffic.

Exhibit Analysis: The Secure Internet Access policy exhibit clearly shows the toggle for Force Certificate Inspection is enabled (set to "ON"). As specified in the Fortinet technical documentation, enabling this option forces the policy to use Certificate Inspection only, overriding any Deep Inspection settings that might be defined in the Profile Group.

Conclusion: Because the traffic is only undergoing certificate-level inspection, the antivirus engine cannot analyze the encrypted eicar.com-zip file payload, allowing the download to proceed even though an antivirus profile is active in the group.

Question: 2

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

A. Allow

B. Pass

C. Permit

D. Exempt

Answer: D

Explanation:

To block all video and audio application traffic while granting access to videos from CNN, you need to configure an application override action in the Application Control with Inline-CASB. Here is the step- by-step detailed explanation:

Application Control Configuration:

Application Control is used to identify and manage application traffic based on predefined or custom application signatures.

Inline-CASB (Cloud Access Security Broker) extends these capabilities by allowing more granular control over cloud applications.

Blocking Video and Audio Applications:

To block all video and audio application traffic, you can create a policy within Application Control to deny all categories related to video and audio streaming.

Granting Access to Specific Videos (CNN):

To allow access to videos from CNN specifically, you must create an override rule within the same Application Control profile.

The override action "Exempt" ensures that traffic to specified URLs (such as those from CNN) is not subjected to the blocking rules set for other video and audio traffic.

Configuration Steps:

Navigate to the Application Control profile in the FortiSASE interface.

Set the application categories related to video and audio streaming to "Block."

Add a new override entry for CNN video traffic and set the action to "Exempt."

Reference:

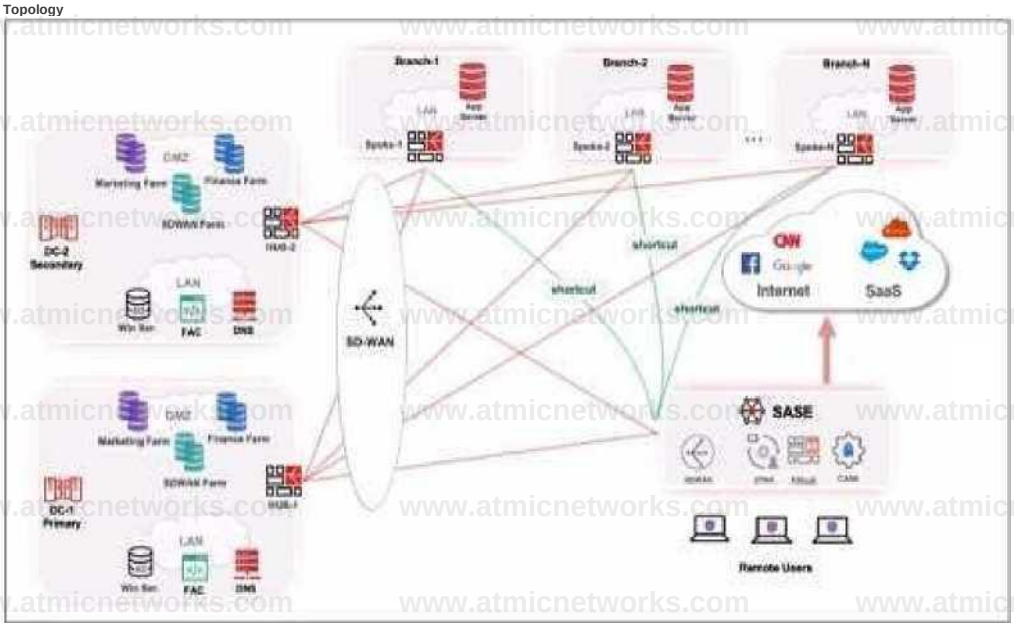
FortiOS 7.6 Administration Guide: Detailed steps on configuring Application Control and Inline-CASB.

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

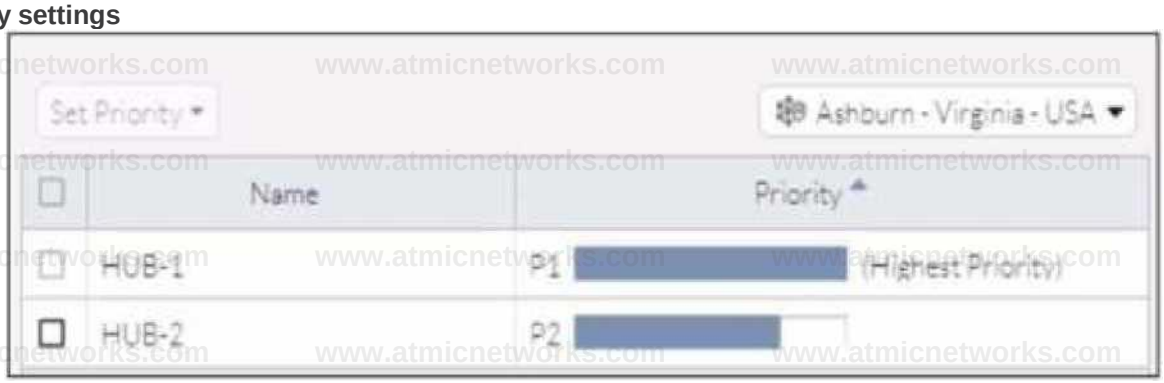
Question: 3

Refer to the exhibits.

Topology



Priority settings



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:

FortiSASE leverages SD-WAN to optimize traffic routing based on performance metrics and priorities.

In the priority settings, HUB-1 is configured with the highest priority (P1), whereas HUB-2 has a lower priority (P2).

Traffic Routing Decision:

FortiSASE evaluates the available hubs (HUB-1 and HUB-2) and selects HUB-1 due to its highest priority setting.

Once the traffic reaches HUB-1, it is then routed to the appropriate branch based on internal routing policies.

Branch-2 Access:

Since HUB-1 has the highest priority, FortiSASE directs the traffic to HUB-1.

HUB-1 then routes the traffic to Branch-2, providing the remote users access to the internal resources.

Reference:

FortiOS 7.6 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.

Question: 4

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):

Zero-trust tags can be used to define policies that either allow or deny access to specific network resources based on the tag associated with the user or device.

This granular control ensures that only authorized users or devices with the appropriate tags can access sensitive resources, thereby enhancing security.

Determining Security Posture:

Zero-trust tags can be utilized to assess and determine the security posture of an endpoint.

Based on the assigned tags, FortiSASE can evaluate the device's compliance with security policies, such as antivirus status, patch levels, and configuration settings.

Devices that do not meet the required security posture can be restricted from accessing the network or given limited access.

Reference:

FortiOS 7.6 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.

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:

When log anonymization is turned on, the actual usernames are replaced with random characters to protect user privacy.

This feature can be beneficial in certain environments but can cause issues when detailed user

monitoring is required.

Disabling Log Anonymization:

Navigate to the FortiSASE settings.

Locate the log settings section.

Disable the log anonymization feature to ensure that actual usernames are displayed in the logs and user connection monitors.

Reference:

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.

Question: 6

Refer to the exhibit.

To allow access, which web tiller configuration must you change on FortiSASE?

A. FortiGuard category-based filter

B. content filter

C. URL Filter

D. inline cloud access security broker (CASB) headers

Answer: C

Explanation:

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

URL Filtering:

URL filtering allows administrators to define policies that block or allow access to specific URLs or URL patterns.

In this case, the URL filter is set to block any URL containing the word "fight."

Modifying URL Filter:

Navigate to the Web Filter configuration in FortiSASE.

Locate the URL filter settings.

Add an exception for the URL https://www.bbc.com/ to allow access, even if it contains a banned word.

Alternatively, remove or adjust the banned word list to exclude the word "fight" if it's not critical to the security policy.

Reference:

FortiOS 7.6 Administration Guide: Provides details on configuring and managing URL filters.

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

Question: 7

Which policy type is used to control traffic between the FortiClient endpoint to FortiSASE for secure internet access?

A. VPN policy

B. thin edge policy

C. private access policy

D. secure web gateway (SWG) policy

Answer: D

Explanation:

The Secure Web Gateway (SWG) policy is used to control traffic between the FortiClient endpoint and FortiSASE for secure internet access. SWG provides comprehensive web security by enforcing policies that manage and monitor user access to the internet.

Secure Web Gateway (SWG) Policy:

SWG policies are designed to protect users from web-based threats and enforce acceptable use policies.

These policies control and monitor user traffic to and from the internet, ensuring that security protocols are followed.

Traffic Control:

The SWG policy intercepts all web traffic, inspects it, and applies security rules before allowing or blocking access.

This policy type is crucial for providing secure internet access to users connecting through FortiSASE.

Reference:

FortiOS 7.6 Administration Guide: Details on configuring and managing SWG policies.

FortiSASE 23.2 Documentation: Explains the role of SWG in securing internet access for endpoints.

Question: 8

Which role does FortiSASE play in supporting zero trust network access (ZTNA) principles9

A. It offers hardware-based firewalls for network segmentation.

B. It integrates with software-defined network (SDN) solutions.

C. It can identify attributes on the endpoint for security posture check.

D. It enables VPN connections for remote employees.

Answer: C

Explanation:

FortiSASE supports zero trust network access (ZTNA) principles by identifying attributes on the endpoint for security posture checks. ZTNA principles require continuous verification of user and device credentials, as well as their security posture, before granting access to network resources.

Security Posture Check:

FortiSASE can evaluate the security posture of endpoints by checking for compliance with security policies, such as antivirus status, patch levels, and configuration settings.

This ensures that only compliant and secure devices are granted access to the network.

Zero Trust Network Access (ZTNA):

ZTNA is based on the principle of "never trust, always verify," which requires continuous assessment of user and device trustworthiness.

FortiSASE plays a crucial role in implementing ZTNA by performing these security posture checks and enforcing access control policies.

Reference:

FortiOS 7.6 Administration Guide: Provides information on ZTNA and endpoint security posture checks.

FortiSASE 23.2 Documentation: Details on how FortiSASE implements ZTNA principles.

Question: 9

When deploying FortiSASE agent-based clients, which three features are available compared to an agentless solution? (Choose three.)

A. Vulnerability scan

B. SSL inspection

C. Anti-ransomware protection

D. Web filter

E. ZTNA tags

Answer: ABD

Explanation:

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

Vulnerability Scan:

Agent-based clients can perform vulnerability scans on endpoints to identify and remediate security weaknesses.

This proactive approach helps to ensure that endpoints are secure and compliant with security policies.

SSL Inspection:

Agent-based clients can perform SSL inspection to decrypt and inspect encrypted traffic for threats.

This feature is critical for detecting malicious activities hidden within SSL/TLS encrypted traffic.

Web Filter:

Web filtering is a key feature available with agent-based clients, allowing administrators to control and monitor web access.

This feature helps enforce acceptable use policies and protect users from web-based threats.

Reference:

FortiOS 7.6 Administration Guide: Explains the features and benefits of deploying agent-based clients.

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

Question: 10

Which FortiSASE feature ensures least-privileged user access to all applications?

A. secure web gateway (SWG)

B. SD-WAN

C. zero trust network access (ZTNA)

D. thin branch SASE extension

Answer: C

Explanation:

Zero Trust Network Access (ZTNA) is the FortiSASE feature that ensures least-privileged user access to all applications.

ZTNA operates on the principle of "never trust, always verify," providing secure access based on the identity of users and devices, regardless of their location.

Zero Trust Network Access (ZTNA):

ZTNA ensures that only authenticated and authorized users and devices can access applications.

It applies the principle of least privilege by granting access only to the resources required by the user, minimizing the potential for unauthorized access.

Implementation:

ZTNA continuously verifies user and device trustworthiness and enforces granular access control policies.

This approach enhances security by reducing the attack surface and limiting lateral movement within the network.

Reference:

FortiOS 7.6 Administration Guide: Provides detailed information on ZTNA and its role in ensuring least-privileged access.

FortiSASE 23.2 Documentation: Explains the implementation and benefits of ZTNA within the FortiSASE environment.

Question: 11

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: A, B

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.

Reference:

FortiOS 7.6 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: 12

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:

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.

Reference:

FortiOS 7.6 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: 13

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:

Hashing data involves converting it into a fixed-size string of characters, which is typically a hash value.

Salting adds random data to the input of the hash function, ensuring that even identical inputs produce different hash values.

This method provides enhanced security by making it more difficult to reverse-engineer the original data from the hash value.

Security and Privacy:

Using salted hashes ensures that user information remains secure and private when stored or analyzed in logs.

This technique is widely used in security systems to protect sensitive data from unauthorized access.

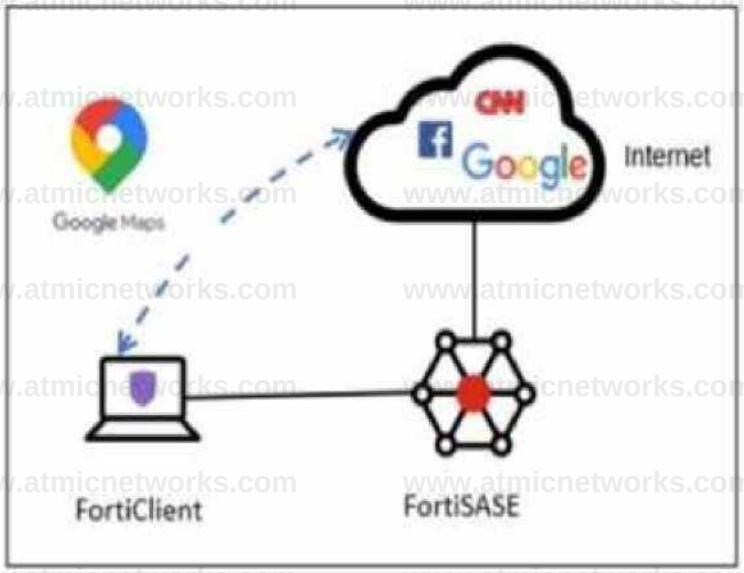
Reference:

FortiOS 7.6 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.

Question: 14

Refer to the exhibit.



A company has a requirement to inspect all the endpoint internet traffic on FortiSASE, and exclude Google Maps traffic from the FortiSASE VPN tunnel and redirect it to the endpoint physical Interface.

Which configuration must you apply to achieve this requirement?

A. Exempt the Google Maps FQDN from the endpoint system proxy settings.

B. Configure a static route with the Google Maps FQDN on the endpoint to redirect traffic

C. Configure the Google Maps FQDN as a split tunneling destination on the FortiSASE endpoint profile.

D. Change the default DNS server configuration on FortiSASE to use the endpoint system DNS.

Answer: C

Explanation:

To meet the requirement of inspecting all endpoint internet traffic on FortiSASE while excluding Google Maps traffic from the FortiSASE VPN tunnel and redirecting it to the endpoint's physical interface, you should configure split tunneling. Split tunneling allows specific traffic to bypass the VPN tunnel and be routed directly through the endpoint's local interface.

Split Tunneling Configuration:

Split tunneling enables selective traffic to be routed outside the VPN tunnel.

By configuring the Google Maps Fully Qualified Domain Name (FQDN) as a split tunneling destination, you ensure that traffic to Google Maps bypasses the VPN tunnel and uses the endpoint's local interface instead.

Implementation Steps:

Access the FortiSASE endpoint profile configuration.

Add the Google Maps FQDN to the split tunneling destinations list.

This configuration directs traffic intended for Google Maps to bypass the VPN tunnel and be routed directly through the endpoint's physical network interface.

Reference:

FortiOS 7.6 Administration Guide: Provides details on split tunneling configuration.

FortiSASE 23.2 Documentation: Explains how to set up and manage split tunneling for specific destinations.

Question: 15

Refer to the exhibits.

WiMO-Pro and Win7-Pro are endpoints from the same remote location. WiMO-Pro can access the internet though FortiSASE, while Wm7-Pro can no longer access the internet

Given the exhibits, which reason explains the outage on Wm7-Pro?

A. The Win7-Pro device posture has changed.

B. Win7-Pro cannot reach the FortiSASE SSL VPN gateway

C. The Win7-Pro FortiClient version does not match the FortiSASE endpoint requirement.

D. Win-7 Pro has exceeded the total vulnerability detected threshold.

Answer: D

Explanation:

Based on the provided exhibits, the reason why the Win7-Pro endpoint can no longer access the internet through FortiSASE is due to exceeding the total vulnerability detected threshold. This threshold is used to determine if a device is compliant with the security requirements to access the network.

Endpoint Compliance:

FortiSASE monitors endpoint compliance by assessing various security parameters, including the number of vulnerabilities detected on the device.

The compliance status is indicated by the ZTNA tags and the vulnerabilities detected.

Vulnerability Threshold:

The exhibit shows that Win7-Pro has 176 vulnerabilities detected, whereas Win10-Pro has 140 vulnerabilities.

If the endpoint exceeds a predefined vulnerability threshold, it may be restricted from accessing the network to ensure overall network security.

Impact on Network Access:

Since Win7-Pro has exceeded the vulnerability threshold, it is marked as non-compliant and subsequently loses internet access through FortiSASE.

The FortiSASE endpoint profile enforces this compliance check to prevent potentially vulnerable devices from accessing the internet.

Reference:

FortiOS 7.6 Administration Guide: Provides information on endpoint compliance and vulnerability management.

FortiSASE 23.2 Documentation: Explains how vulnerability thresholds are used to determine endpoint compliance and access control.

Question: 16

A customer wants to upgrade their legacy on-premises proxy to a could-based proxy for a hybrid network. Which FortiSASE features would help the customer to achieve this outcome?

A. SD-WAN and NGFW

B. SD-WAN and inline-CASB

C. zero trust network access (ZTNA) and next generation firewall (NGFW)

D. secure web gateway (SWG) and inline-CASB

Answer: D

Explanation:

For a customer looking to upgrade their legacy on-premises proxy to a cloud-based proxy for a hybrid network, the combination of Secure Web Gateway (SWG) and Inline Cloud Access Security Broker (CASB) features in FortiSASE will provide the necessary capabilities.

Secure Web Gateway (SWG):

SWG provides comprehensive web security by inspecting and filtering web traffic to protect against web-based threats.

It ensures that all web traffic, whether originating from on-premises or remote locations, is inspected and secured by the cloud-based proxy.

Inline Cloud Access Security Broker (CASB):

CASB enhances security by providing visibility and control over cloud applications and services.

Inline CASB integrates with SWG to enforce security policies for cloud application usage, preventing unauthorized access and data leakage.

Reference:

FortiOS 7.6 Administration Guide: Details on SWG and CASB features.

FortiSASE 23.2 Documentation: Explains how SWG and inline-CASB are used in cloud-based proxy solutions.

Question: 17

When you configure FortiSASE Secure Private Access (SPA) with SD-WAN integration, you must establish a routing adjacency between FortiSASE and the FortiGate SD-WAN hub. Which routing protocol must you use?

A. BGP

B. IS-IS

C. OSPF

D. EIGRP

Answer: A

Explanation:

When configuring FortiSASE Secure Private Access (SPA) with SD-WAN integration, establishing a routing adjacency between FortiSASE and the FortiGate SD-WAN hub requires the use of the Border Gateway Protocol (BGP).

BGP (Border Gateway Protocol):

BGP is widely used for establishing routing adjacencies between different networks, particularly in SD-WAN environments.

It provides scalability and flexibility in managing dynamic routing between FortiSASE and the FortiGate SD-WAN hub.

Routing Adjacency:

BGP enables the exchange of routing information between FortiSASE and the FortiGate SD-WAN hub.

This ensures optimal routing paths and efficient traffic management across the hybrid network.

Reference:

FortiOS 7.6 Administration Guide: Provides information on configuring BGP for SD-WAN integration.

FortiSASE 23.2 Documentation: Details on setting up routing adjacencies using BGP for Secure Private Access with SD-WAN.

Question: 18

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:

This step allows FortiSASE to recognize and establish a connection with the corporate FortiGate.

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

The EMS (Endpoint Management Server) cloud connector facilitates the integration between FortiClient endpoints and FortiSASE, enabling seamless sharing of endpoint information.

Register FortiGate and FortiSASE under the same FortiCloud account:

By registering both FortiGate and FortiSASE under the same FortiCloud account, you ensure centralized management and synchronization of configurations and policies.

Reference:

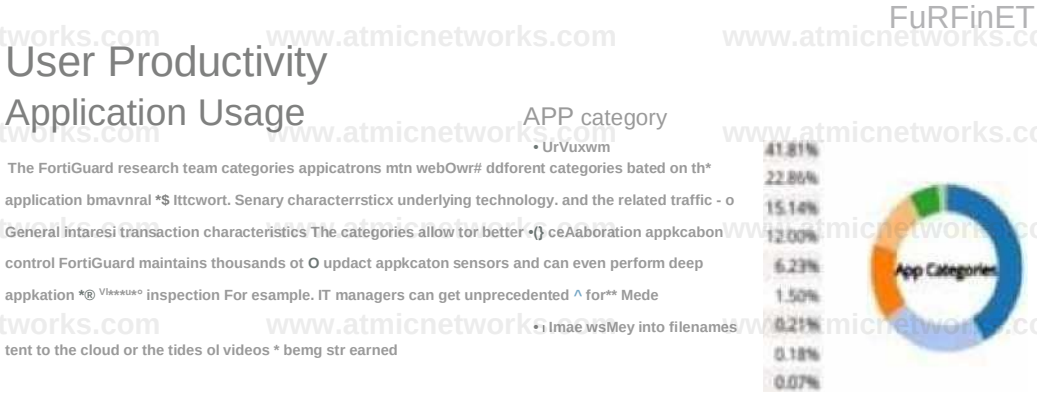
FortiOS 7.6 Administration Guide: Provides details on configuring Secure Private Access and integrating with FortiGate.

FortiSASE 23.2 Documentation: Explains how to set up and manage connections between FortiSASE and corporate FortiGate.

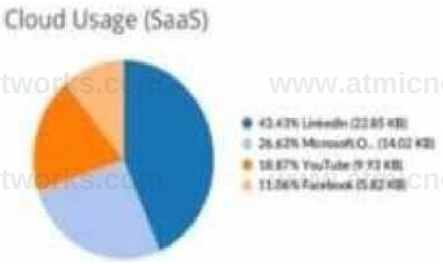
Question: 19

Refer to the exhibit.

Daily report for application usage



With the profiler anon of cloud-based computing enterprises are mcreasMtgly reliant on Chad parties for infrastructure plumbing Unfortunately for enterprises des meant that thee reformation it only at tecure at the cfoud provider s security to addfoon, it can often introduce redundancy lit services are already erasable tntemady) and nr crave cma llf not rnontlored property)



IT managers are often unaware of how many cloud based services are in use wehm their organization Sometimes, these applications can be used to uruerwent or even replace corporate erfrauructure already available to users In leu erf ease of use unfortunate^ a potential side effect of this is that yoca sensitive corporate information could be transferred to the cloud Accordingly your data could be exposed f the cloud powder's security infrastructure a breached

The adoption ol Infrastructure at a senate' (1aaS) platforms a popular and can be wry metal when compute resource* are tinted or hare spesukted reguvemerts That tael the elective outsourcing of your eifrattructure must be wee regscated to prevent misuse The occasional audting ol laaS appscanons can be a usefU eee>cac not only lor security purposes, but also to merenue organcationai costs associated with pay per use models or reciamg subscription lees

Cloud Usage (IaaS)

No matching fog data for tMt report

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: B, D

Explanation:

In FortiSASE, the accuracy of application usage reports depends on two primary factors: the ability to identify the application (visibility) and the configuration to log that data (reporting).

Deep Inspection Requirement (D): Modern applications frequently use encryption (SSL/TLS) and dynamic ports. Without Deep Inspection (SSL decryption), the FortiSASE security engine cannot see the application payload and is limited to inspecting headers or SNI. This results in many applications being identified only by their generic protocol (e.g., "SSL" or "HTTPS") and subsequently appearing as Unknown in reports because the specific Layer 7 application signature cannot be matched.

Application Control Monitor Setting (B): Even when an application is correctly identified, it must be properly logged to appear accurately in the "Daily report for application usage". In the inline-CASB (Application Control) profile, categories are assigned actions such as "Allow", "Block", or "Monitor". If categories are set to "Allow" instead of Monitor, the traffic is permitted but granular session details—including the specific application category—may not be logged for reporting purposes, causing them to be grouped into an "Unknown" or "Uncategorized" bucket in high-level summaries.

Analysis of Incorrect Options:

Option A: While certificate inspection provides more visibility than no inspection, it is still insufficient for many applications that require deep packet inspection for identification. Therefore, the lack of Deep inspection (Option D) is the more accurate technical explanation for "Unknown" results.

Option C: ZTNA tags are used for access control and posture-based policy enforcement; they do not impact the application identification engine's ability to categorize traffic flows.

Question: 20

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?

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.

Reference:

FortiOS 7.6 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.

Question: 21

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

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.

Reference:

FortiOS 7.6 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: 22

Refer to the exhibits.

VPN tunnel diagnose output on FortiGate Hub

```
• diagnose vpn tunnel Hit nene SASE.9
Hit ipsec tunnel by nenes in vd 8

none-SASE 8 ver-2 serial-14 172.16 19 191 4588 -172.16 18 1 64916 tun.id-19.il.11.19 tun.id6- 19.9 9 18 det.stu-159 bound.lf*4 lgwy-atatic/1 tun-intf node-dial.1nst/3 eric ep-none/74664
optional123a8|-npu rgey-chg rport-chg frag-rfc d>1M
pa rent-SASE lhdex-9
 proxyid.nun-1 child.nua»8 refcnt-7 ilaat-9 olast-9 ad-a/1 atat rap-1667 tap-4583 rxb-278576 tab-199695
 dpd: node-on-idle on-1 idle-2990taa retry-) count-9 seqno-1 natt: node*keepalive draft-9 interval-18 renote.port-64916 fee: egress-9 ingreai-9
proayid*SASE proto-9 aa-1 ref-4 ter lai-1 ads
    ■re: 9:9.9.9.9-255 25S.25S.265:9 dit: 9:9 9 9 9 255 255 255 255 9 S* ref-6 optlona-a26 type-99 aoft-9 atu*1422 eipire-42925/99 replaywin-1924 seqno-11cf esn-9 replaywin lastaeq-
   88998688 qat-B rekey-9 haah.search_len»1 life: type-91 bytes-8/9 tuaeout-43189/43299 dec. spl-6934f978 eap-eea key-16 2e89329989l7c1fdeed9242673bc76fS ah-she1 key-29
   91b6c2a13e6cff22796e428c5fMe4c5262b1a71
    enc api-fl6ee4a1 esp-aes key-16 99dce5d6Mcaf2714a4f84cff482b557 ah-eha1 key-29 b69cdec39489a9f599fo729cec9o36bb92Mf824
    dec pkti/bytes-3/129. enc pkts/bytes-2599/2B5776 nou.flaq-93 npu.rqwy-172.16 19.1 nou.lqwy-172.16 19.191 npu.aelid-11 dec.npuid-1 enc npuid>1
```

Secure Private Access policy on FortiSASE

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:

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.

Reference:

FortiOS 7.6 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: 23

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):

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.

Reference:

FortiOS 7.6 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: 24

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

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.

Reference:

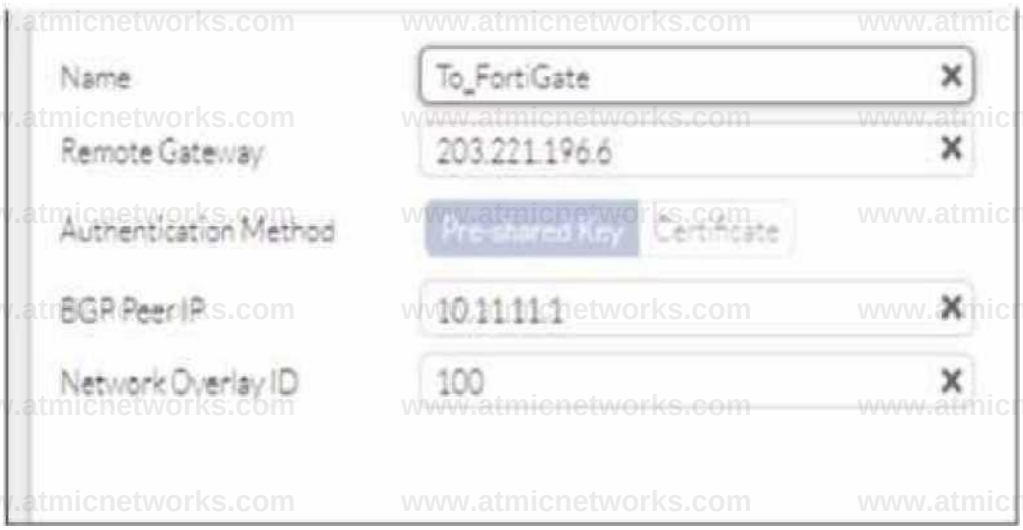
FortiOS 7.6 Administration Guide: Details on different SIA deployment use cases and configurations.

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

Question: 25

Refer to the exhibits.

Secure private access service connection



3GP protocol configuration

```
Sconfig router bgp set as 65861 set router-id 10.1.6.254 config neighbor
        edit '16.18.1.3' set advertisement-internal 1 *et ebgp-enforce-oiultihop enable set link-down-failover
            enable set remote-as 5500'
                set route-ref lector-client enable nert
    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 5500'
                        set  additional-path both
```

```
set adv-additional-path 4
set route-reflector-client enable
nert end config neighbor-range edit 1
set prefix 18.11.11.8 255.255.255.0 set neighbor-group *To_5ASC* next end config network edit 1
set prefix 10.190.'90.0 255.255.255.0 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.

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.

Reference:

FortiOS 7.6 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: 26

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: 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.

Reference:

FortiOS 7.6 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: 27

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.

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.

Reference:

FortiOS 7.6 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: 28

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: 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.

Reference:

FortiOS 7.6 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: 29

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

A. 3

B. 4

C. 2

D. 1

Answer: D

Explanation:

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

Security Point of Presence (PoP):

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.

Reference:

FortiOS 7.6 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: 30

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 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.

Reference:

FortiOS 7.6 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: 31

Which authentication method overrides any other previously configured user authentication on FortiSASE?

A. Local

B. SSO

C. RADIUS

D. MFA

Answer: B

Explanation:

Comprehensive and Detailed Explanation From FortiSASE 24.x/25.x, FortiOS 7.4, FortiAuthenticator 6.5, FortiClient 7.0 and later Exact Extract study guide:

In FortiSASE environments, Single Sign-On (SSO) is prioritized as the primary enterprise authentication mechanism. According to the FortiSASE Configuration Guide and Security Operations documentation, when you configure SAML SSO (Single Sign-On), it serves as a global authentication setting that overrides any previously configured local or remote (RADIUS/LDAP) user authentication methods for the secure web gateway (SWG) and VPN tunnels.

The architectural logic is designed to ensure a seamless "Zero Trust" identity provider (IdP) experience. Once SSO is enabled and configured (typically using Azure AD, Okta, or FortiAuthenticator as the IdP), FortiSASE redirects authentication requests to the defined IdP. This effectively supersedes manual local user databases or legacy RADIUS configurations to maintain a single source of truth for identity management. While MFA is often a component of the authentication process, it is a secondary factor, whereas SSO is the foundational method that dictates the authentication flow and overrides prior settings.

Question: 32

What is the role of ZTNA tags in the FortiSASE Secure Internet Access (SIA) and Secure Private Access (SPA) use cases? (Choose one answer)

A. ZTNA tags are created to isolate browser sessions in SIA and enforce data loss prevention in SPA for all devices.

B. ZTNA tags determine device posture for non-web traffic protocols and are applied only in agentless deployments for SIA.

C. ZTNA tags determine device posture for endpoints running FortiClient and are used to grant or deny access in SIA or SPA based on that posture.

D. ZTNA tags are applied to unmanaged endpoints without FortiClient to secure HTTP and HTTPS traffic in SIA and SPA.

Answer: C

Explanation:

In the Fortinet SASE architecture, Zero Trust Network Access (ZTNA) tags (which have been renamed to Security Posture Tags starting with FortiClient/EMS 7.4.0) play a critical role in continuous posture assessment. These tags are dynamic metadata assign8ed to an endpoint based on specific conditions or "tagging rules" defined in the FortiSASE Endpoint Management Service (EMS).

Posture Determination: The FortiClient agent, installed on the endpoint, monitors the device for various security attributes—such as whether an antivirus is running, the presence of specific registry keys, OS version, or the absence of critical vulnerabilities.

SIA (Secure Internet Access) Use Case: In SIA scenarios, FortiSASE uses these tags within security policies to control internet access. For example, a policy may allow full internet access only to endpoints tagged as "Compliant" while redirecting "Non-Compliant" devices to a restricted remediation portal.

SPA (Secure Private Access) Use Case: In SPA (specifically ZTNA Proxy mode), the tags are synchronized from FortiSASE to the corporate FortiGate (acting as the ZTNA Access Proxy).12 When a user attempts to access a private application, the FortiGate checks the endpoint's client certificate and its synchronized ZTNA tags.13 If the endpoint does not meet the required posture (e.g., it is missing a required "Domain-Joined" tag), access is denied at the session level.

According to the FortiSASE 25 Enterprise Administrator Study Guide, ZTNA tags are fundamental to

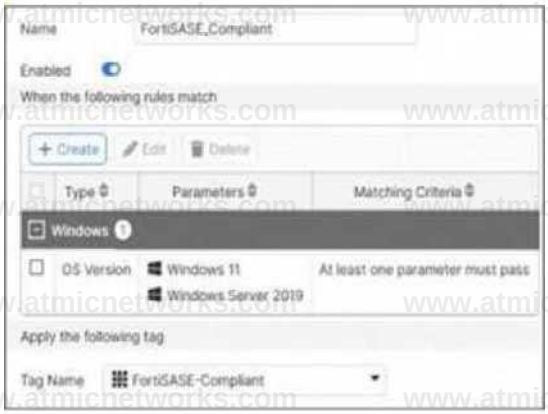
the "Zero Trust" principle because they move beyond static identity (username/password) to verify the real-time security state of the device before granting access to either the internet or internal private resources.

Question: 33

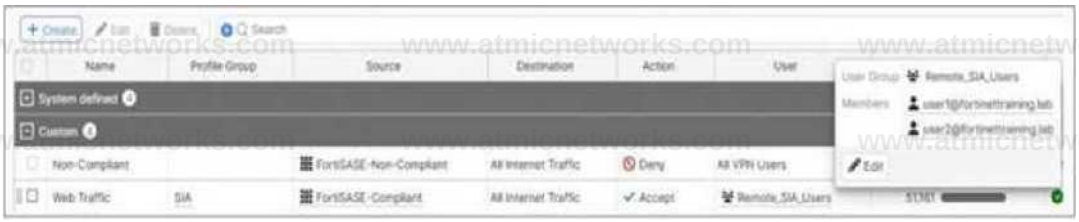
Refer to the exhibits.

Managed Endpoints

ZTNA Tagging Rules



Secure Internet Access Policy



Jumpbox and Windows-AD are endpoints from the same remote location. Jumpbox can access the internet through FortiSASE, while Windows-AD can no longer access the internet. Based on the information in the exhibits, which reason explains the outage on Windows-AD? (Choose one answer)

A. The device security posture for Windows-AD has changed.

B. The FortiClient version installed on Windows-AD does not match the expected version on FortiSASE.

C. Windows-AD is excluded from FortiSASE management.

D. The remote VPN user on Windows-AD no longer matches any VPN policy.

Answer: A

Explanation:

In FortiSASE, Zero Trust Network Access (ZTNA) tags—also known as security posture tags—are used to dynamically grant or deny access based on the real-time security state of an endpoint. This mechanism ensures that only devices meeting specific compliance requirements can access protected resources or the internet.

Endpoint Analysis: The Managed Endpoints exhibit shows that while Jumpbox only has the FortiSASE-Compliant tag, the Windows-AD endpoint has been assigned both FortiSASE-Compliant and FortiSASE-Non-Compliant tags. This indicates that a security posture check on the Windows-AD device has failed, triggering a rule that applies the non-compliant tag.

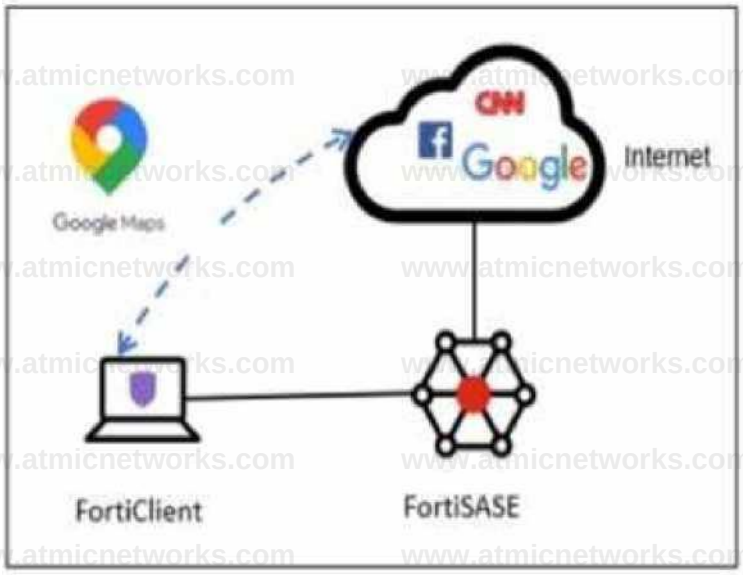
Policy Evaluation: The Secure Internet Access Policy table shows two custom policies. The first policy, named Non-compliant, uses the FortiSASE-Non-Compliant tag as its source and has the action set to Deny. The second policy, Web Traffic, allows access for FortiSASE-Compliant users.

Root Cause of Outage: Because FortiSASE (powered by FortiOS) processes security policies in a topdown sequence, the "Non-compliant" policy is evaluated first. Since Windows-AD matches the source criteria for this "Deny" policy, its traffic is blocked before it can reach the "Accept" policy.

Although the exhibit shows a warning icon for the FortiClient version on Windows-AD, the direct cause of the internet outage is the explicit Deny policy triggered by the change in the device's security posture (the application of the Non-Compliant tag).

Question: 34

Refer to the exhibit.



An organization must inspect all the endpoint internet traffic on FortiSASE, and exclude Google Maps traffic from the FortiSASE tunnel and redirect it to the endpoint physical interface.

Which configuration must you apply to achieve this requirement? (Choose one answer)

A. Add the Google Maps URL in the zero trust network access (ZTNA) TCP access proxy forwarding rule.

B. Configure a steering bypass tunnel firewall policy using Google Maps FQDN to exclude and redirect the traffic.

C. Exempt Google Maps in URL filtering in the web filter profile.

D. Add the Google Maps URL as a steering bypass destination in the endpoint profile.

Answer: D

Explanation:

In FortiSASE, the requirement to redirect specific traffic away from the secure tunnel and through the local physical interface is achieved through Steering Bypass (commonly referred to as split tunneling).

Steering Bypass Destinations: This feature is configured within the Endpoint Profile settings. When an administrator adds a destination (such as the Google Maps URL or FQDN) to the Steering Bypass table, the FortiClient agent updates the local routing table on the endpoint.

Traffic Redirection: Traffic matching these bypass rules is explicitly excluded from the FortiSASE VPN tunnel and instead sent directly out of the device's local internet gateway (physical interface). This is ideal for optimizing bandwidth and reducing latency for trusted, high-volume applications like mapping services or video conferencing.

Analysis of Other Options:

Option A: ZTNA TCP access proxy rules are designed for secure access to private applications, not for managing how internet-bound traffic is routed.

Option B: While it uses the term "steering bypass," there is no "tunnel firewall policy" configuration for this purpose; the configuration is done at the endpoint profile level.

Option C: Exempting a URL in the Web Filter profile only instructs FortiSASE to skip security scanning (AV, DLP, etc.) for that traffic. The traffic would still be encapsulated in the tunnel and sent to FortiSASE, which does not meet the requirement to redirect it to the physical interface.

By configuring the Google Maps URL as a steering bypass destination, the organization ensures the traffic never enters the SASE tunnel, fulfilling the requirement for both traffic inspection (for all other traffic) and local redirection (for Google Maps).

Question: 35

DRAG DROP

When configuring the DLP rule in FortiSASE using Regex format, what would be the correct order for the configuration steps? (Place the four correct steps in order)

Answer:

Explanation:

1. DLP Data Pattern
2. DLP Dictionary
3. DLP Sensor
4. DLP Profile

The FortiSASE Data Loss Prevention (DLP) framework follows a hierarchical object-oriented structure. When creating a custom DLP rule using Regular Expressions (Regex), the administrator must build the components from the most granular level upward to the policy level.

DLP Data Pattern: This is the first step where the actual Regex string is defined. The pattern specifies what specific data string (e.g., a specific credit card format or employee ID) the engine should look for.

DLP Dictionary: Once the pattern is created, it must be added to a Dictionary. The dictionary acts as a container that groups one or more data patterns together for easier management.

DLP Sensor: The dictionary is then linked to a DLP Sensor. Within the sensor, you define the "Rule" which specifies the dictionary to use and the action to take (such as block, log, or quarantine) when a match occurs.

DLP Profile: Finally, the sensor is applied to a DLP Profile. This profile is the high-level object that is ultimately selected within a FortiSASE Security Policy to inspect traffic for sensitive data.

Question: 36

Refer to the exhibits.

Traffic logs

Log Details

Details Security

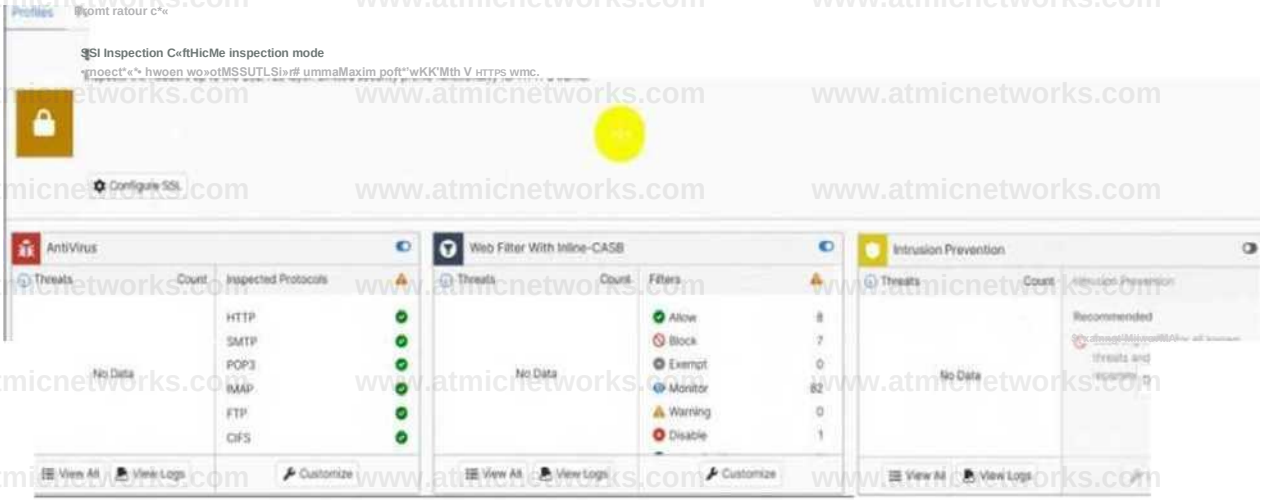
0 **'Met> Finer wnh mine-CASB** **S A**

Category	SO
Category Description	Information and Computer Security
Direction	outgoing
Event Type	ftgd.allow
Hostname	www.eKar.org
Message	URL belongs to an allowed category If policy
Profile Group	A Default (internet Access]
Request Type	deed
Source Domain	trainingAD training lab
Sub Type	wobblier
Type	utm
Timezone	•0000
Unauthenticated User Source	forticllent
URL	httpsJ/www eicar.org/

□ **Application Control With Inline CASB** **~ i**

Direction	incoming
Event Type	signature
Hostname	www.ecar org
Incident Serial No	36709018
Message	Web.CUent HTTPS BROWSER
Source Domain	ttainmgAO training lab
Sub Typo	app-ctri
Type	utm
Timezone	•OOOO
Unauthenlicatcd User Source	lorticlient
URL	/

Security profile group



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.

Which configuration on FortiSASE is allowing users to perform the download? (Choose one answer)

A. Deep inspection is not enabled.

B. Application control is exempting all the browser traffic.

C. Web filter is allowing the URL.

D. Intrusion prevention is disabled.

Answer: A

Explanation:

The core of the issue shown in the exhibits is the lack of visibility into encrypted traffic.

HTTPS Encryption: The eicar.org website uses the HTTPS protocol for its downloads. This means the data payload, including the test malware file, is encrypted as it traverses the network.

SSL Inspection Modes: As seen in the Security profile group exhibit (image_5705fc.jpg), the SSL inspection mode is explicitly set to Certificate inspection mode.

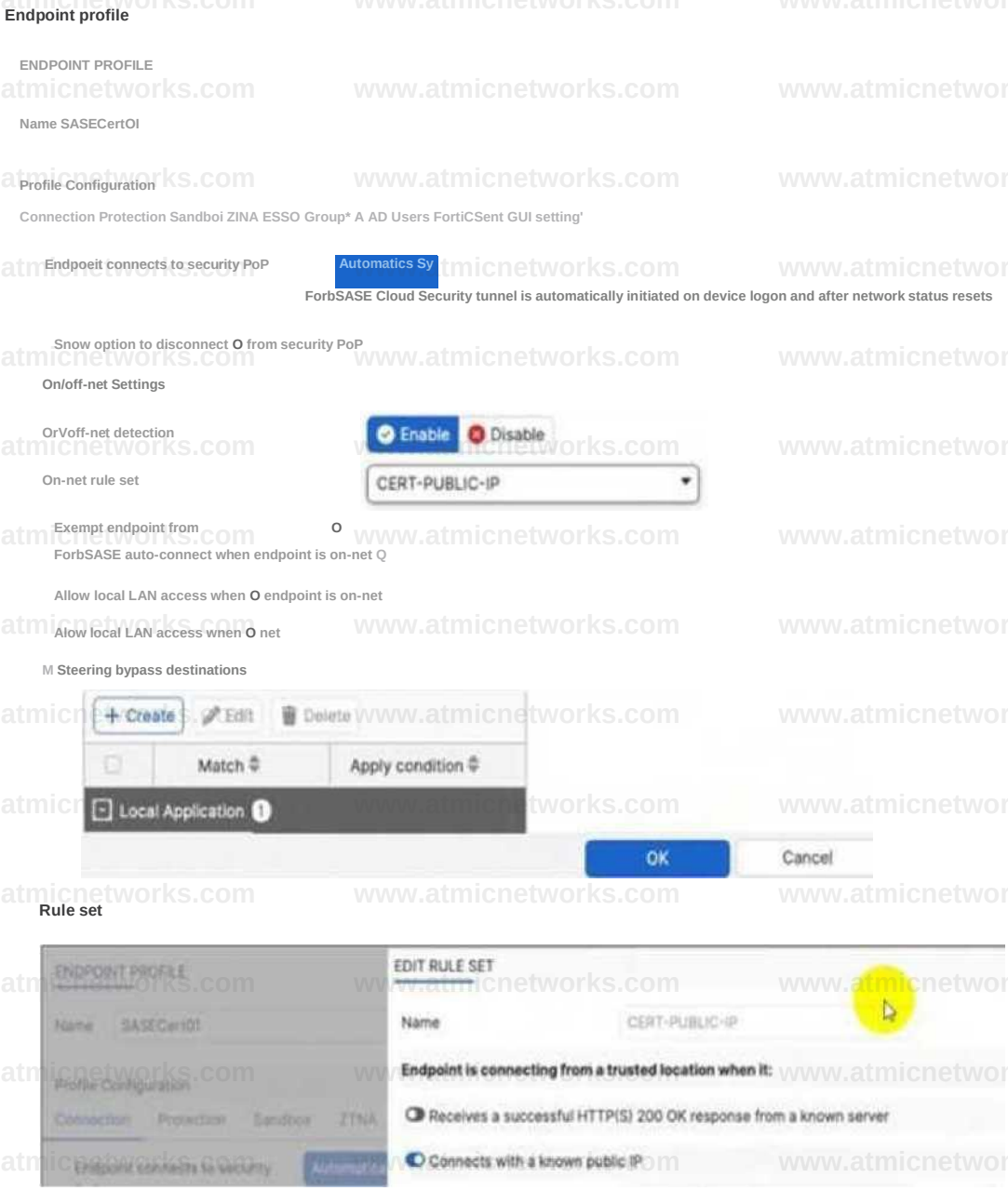
Visibility Gap: Certificate inspection only analyzes the initial SSL handshake, such as the server certificate and SNI (Server Name Indication). It does not decrypt the traffic payload. Consequently, the antivirus engine in FortiSASE cannot "see" or scan the eicar.com-zip file hidden within the encrypted session.

Resolution Requirement: To detect and block malicious files over HTTPS, SSL Deep Inspection must be enabled. Deep inspection allows FortiSASE to act as a proxy, decrypting the traffic for full content scanning by the antivirus and IPS engines before re-encrypting it for the endpoint.

Log Analysis: While the web filtering logs (image_5704e5.jpg) show the traffic is "Allowed" because the URL is not blocked by a web filter category, this is only the first step of inspection. The antivirus engine is present but ineffective because it is blind to the encrypted content due to the lack of deep inspection.

Question: 37

A customer configured the On/off-net detection rule to disable FortiSASE VPN auto-connect when users are inside the corporate network. The rule is set to Connects with a known public IP using the company's public IP address. However, when the users are on the corporate network, the FortiSASE VPN still auto-connects. The customer has confirmed that traffic is going to the internet with the correct IP address.



Which configuration is causing the issue? (Choose one answer)

A. The On-net rule set configuration is incorrect.

B. Allow local LAN access when endpoint is on-net is disabled when it should be enabled.

C. Exempt endpoint from FortiSASE auto-connect is disabled when it should be enabled.

D. Is connected to a known DNS server should be enabled and configured.

Answer: C

Explanation:

The FortiSASE On/off-net detection feature is a two-part configuration designed to optimize bandwidth and user experience by determining when a device is in a trusted environment.

Rule Set Definition: The first part involves defining what constitutes an "on-net" or "on-fabric" status. In this scenario, the customer successfully configured a rule set named CERT-PUBLIC-IP using the Connects with a known public IP detection type. This tells FortiSASE that if the endpoint's public WAN IP matches the corporate gateway, it is considered to be on the corporate network.

Profile Exemption Logic: Defining the rule set is not enough to stop the VPN connection. Within the Endpoint Profile (under the Connection tab > On/off-net Settings), there is a specific toggle labeled Exempt endpoint from FortiSASE auto-connect when endpoint is on-net (or in some versions, Bypass FortiSASE when endpoint is on-net).

Exhibit Analysis: Looking at the provided exhibit (image_57097d.jpg), the "Exempt endpoint from FortiSASE auto-connect..." toggle is clearly disabled (switched to the left).

Root Cause: Because this toggle is disabled, FortiClient identifies that it is "on-net" based on the IP rule, but it has no instruction to skip the VPN connection. Consequently, the "Automatically" initiate tunnel setting remains the dominant instruction, causing the VPN to connect regardless of the network location.

To resolve the issue, the administrator must enable the Exempt endpoint from FortiSASE autoconnect when endpoint is on-net option in the SASECert01 profile.

Question: 38

How does FortiSASE Secure Private Access (SPA) facilitate connectivity to private resources in a hub- and-spoke network? (Choose one answer)

A. SPA establishes direct links to spokes without IPsec or BGP and uses an easy configuration key to secure web traffic for remote users.

B. SPA applies source network address translation (SNAT) for remote user traffic and uses IKEv1 for IPsec tunnels to connect to standalone hubs without BGP support.

C. SPA connects to private resources using HTTP and HTTPS protocols and relies on FortiClient for agentless access to SD-WAN deployments.

D. SPA connects a FortiSASE POP to a FortiGate hub or SD-WAN deployment using IPsec and BGP for dynamic route exchange with an easy configuration key for simplified setup on FortiOS.1

Answer: D

Explanation:

FortiSASE Secure Private Access (SPA) is designed to provide remote users with seamless and secure access to private applications hosted behind an organization's FortiGate Next-Generation Firewall (NGFW) or SD-WAN hubs.2

Hub-and-Spoke Architecture: In this deployment model, the organization's FortiGate (either a standalone NGFW or an SD-WAN hub) acts as the hub, while the global FortiSASE Security Points of Presence (PoPs) act as spokes.3

IPsec and BGP Integration: The connectivity between the FortiSASE PoPs and the corporate hub is established via IPsec VPN tunnels. To manage routing and ensure that remote users can reach the correct internal subnets, Border Gateway Protocol (BGP) is used for dynamic route exchange.4 This allows the hub to advertise internal prefixes to FortiSASE, enabling the PoPs to route user traffic effectively without requiring complex static route management.

Simplified Configuration: To reduce administrative overhead and prevent manual configuration errors on the FortiOS side, Fortinet introduced the SPA easy configuration key (also known as an invitation code or simplified SPA setup). An administrator generates this key in the FortiSASE portal and enters it on the FortiGate hub. This triggers the Fabric Overlay Orchestrator to automatically provision the necessary IPsec tunnels, BGP peerings, and firewall policies required for SPA connectivity.

According to the FortiSASE 25 Architecture Guide, this method is preferred over legacy VPNs because it supports both TCP and UDP traffic, integrates natively with existing SD-WAN deployments, and automatically finds the shortest path to applications using ADVPN (Auto-Discovery VPN) shortcuts where applicable.

Question: 39

For monitoring potentially unwanted applications on endpoints, which information is available on the FortiSASE software installations page? (Choose two answers)

A. The endpoint the software is installed on1
B. The license status of the software2
C. The vendor of the software3
D. The usage frequency of the software

Answer: A, C

Explanation:

In FortiSASE, the Software Installations page (located under Network > Managed Endpoints) provides a centralized view of all software inventory reported by the FortiClient agents. This feature is essential for administrators to maintain visibility into the environment and identify potentially unwanted applications (PUA) or unauthorized software installed on remote devices.

Software Inventory Reporting: FortiClient sends the endpoint's software inventory to FortiSASE upon initial registration and updates the portal whenever a change—such as an installation, update, or removal—occurs on the endpoint.

Available Information (Vendor): When viewing the global list of applications, the portal displays detailed metadata for each software entry. This includes the Vendor of the software and its specific version, allowing administrators to differentiate between reputable enterprise applications and suspicious third-party utilities.

Available Information (Endpoint Association): The interface includes an Endpoint Count field that indicates how many devices have a specific application installed. By selecting a specific application and using the View Endpoints action, the administrator can see a list of every individual endpoint where that software is currently active.

Incorrect Options: While license management is a general feature of the ecosystem, the Software Installations page itself does not track the license status of individual third-party applications (Option B). Similarly, while FortiSASE monitors traffic, the Software Installations inventory page does not

report on the usage frequency (how often a user opens or uses the app) of the installed binaries (Option D).

By leveraging this inventory, administrators can proactively manage risk by identifying endpoints that possess high-risk

software and taking remediation steps or applying ZTNA posture tags based on the presence of specific unauthorized software.

Question: 40

A Fortinet customer is considering integrating FortiManager with FortiSASE. What are two prerequisites they should consider? (Choose two answers)

A. Adding a FortiManager connection add-on license to FortiSASE.

B. Placing FortiManager in the same FortiCloud account as FortiSASE.

C. Reducing the number of FortiSASE PoPs that support FortiManager.

D. Running a FortiManager version that is supported by FortiSASE.

Answer: B, D

Explanation:

Integrating FortiManager with FortiSASE allows for central management of configuration objects like addresses and5 security 6profiles. For this integration to function correctly, the following key prerequisites must be met:

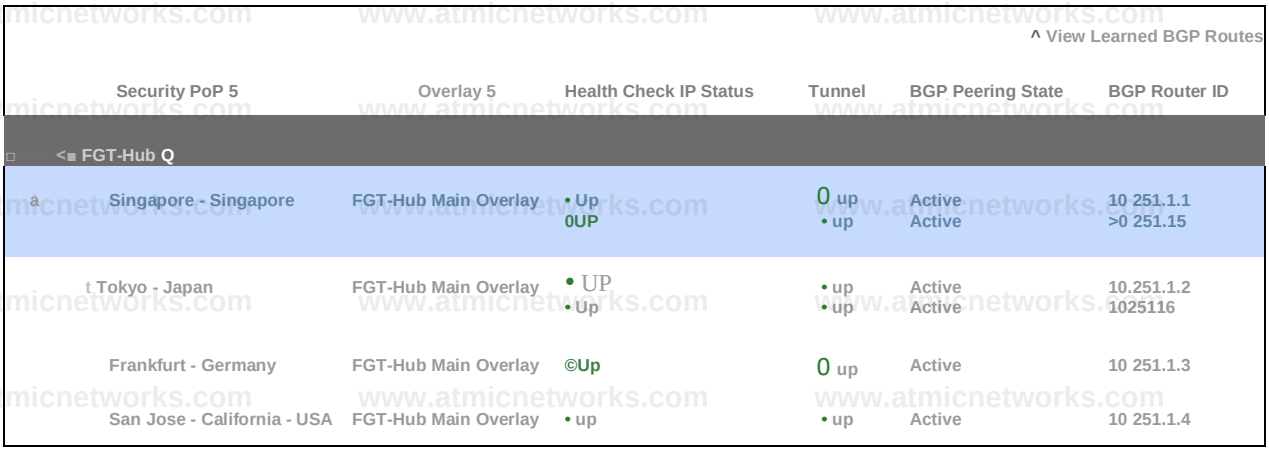
Same FortiCloud Account: A fundamental requirement for the integration is that both 10the FortiSASE instance and the FortiManager (whether physical, VM, or Cloud) must be registered under the same FortiCloud (FortiCare) account. This common identity allows the platforms to securely discover and authorize each other for synchronization.

Supported Firmware Version: The FortiManager must run a firmware version that is compatible with the FortiSASE release. According to the FortiSASE 25 Enterprise Administrator Study Guide, FortiManager version 7.4.4 or later is generally required to support the specific API connectors and object synchronization logic used by current FortiSASE environments. Using an unsupported version may result in synchronization failures or missing configuration features.

Management Logic: Once these prerequisites are met, the administrator can enable "Central Management" in the FortiSASE portal. This creates a one-way synchronization where FortiManager acts as the source of truth for objects like Security Profile Groups, ensuring consistent security posture across both the SASE cloud and on-premises FortiGates.

Question: 41

Refer to the exhibit.



An SPA service connection is experiencing connectivity problems. Which configuration setting should the administrator verify and correct first? (Choose one answer)

A. Remote Gateway

B. BGP Peer IP

C. Network overlay ID

D. Authentication Method

Answer: B

Explanation:

In FortiSASE Secure Private Access (SPA) deployments, establishing a stable connection between the FortiSASE PoPs and the corporate FortiGate hub relies on two primary layers: the IPsec Tunnel and the BGP Peering.

Exhibit Analysis: The exhibit (image_577e17.jpg) shows the status of several Security PoPs (Singapore, Tokyo, Frankfurt, and San Jose) connected to an "FGT-Hub".

Tunnel Status vs. BGP Status: For all listed PoPs, the Health Check IP Status and Tunnel status are both shown with a green "Up" icon. This confirms that the underlying IPsec connectivity and the physical path between the SASE cloud and the hub are functioning correctly.

Identifying the Failure: The BGP Peering State is reported as Active. In BGP terminology, the "Active" state specifically indicates that the router is attempting to initiate a TCP connection with its peer but has not yet received a response. A fully functional and successful BGP connection must reach the Established state.

Root Cause Determination: Since the tunnel is up (eliminating Gateway or Authentication Method issues as the primary suspects) but the BGP state remains stuck in "Active," the most likely cause is a mismatch or misconfiguration in the BGP Peer IP or BGP neighbor settings. This prevents the exchange of routing information necessary for users to access private applications.

To resolve the connectivity problem, the administrator must ensure that the BGP neighbor IPs configured on the FortiGate hub match those assigned by the FortiSASE orchestration and that firewall policies on the hub allow BGP traffic (TCP port 179) across the tunnel.

Question: 42

Refer to the exhibit.

IPAM Configuration

Public IP IPAM

IPAM CONFIGURATION

IP pools for tunnel and edge devices	A 172.16.0.0/12	X
Excluded subnetsQ	172.16.0.0/15	X
	172.18.0.0/15	X
	172.20.0.0/15	X
	172.22.0.0/15	
	172 240.0/15	X
	172.26.0.0/15	X
	172.28.0.0/15	X
	172.30.0.0/15	X

A customer wants to fine-tune network assignments on FortiSASE, so they modified the IPAM configuration as shown in the exhibit. After this configuration, the customer started having connectivity problems and noticed that devices are using excluded ranges. What could be causing the unexpected behavior and connectivity problems? (Choose two answers)

A. The pool mustinclude at least one /20 per security POP for the IPAM to work correctly.

B. The pool mustinclude at least one /16 per Instance for the IPAM to work correctly.

C. The pool mustinclude at least one /20 per Instance for the IPAM to work correctly.

D. The customer excluded too many networks from the pool.

Answer: A, D

Explanation:

IP Address Management (IPAM) in FortiSASE is responsible for automatically allocating subnets to various services, including VPN tunnels and Edge devices. When an administrator modifies the default IPAM configuration, they must adhere to specific architectural scaling requirements.

Subnet Requirements per PoP: FortiSASE architecture requires a minimum amount of address space to be available for each provisioned Security Point of Presence (PoP) to handle internal routing and endpoint assignments. For the IPAM engine to function correctly and distribute unique subnets across the global infrastructure, the pool must provide at least one /20 subnet per security PoP. If the available space is smaller than this per-PoP requirement, the allocation logic may fail or produce unpredictable routing behavior.

Impact of Excessive Exclusions: In the exhibit (image_578940.png), the customer has defined a large summary pool of 172.16.0.0/12. However, they have configured eight separate /15 excluded subnets: 172.16.0.0/15, 172.18.0.0/15, 172.20.0.0/15, 172.22.0.0/15, 172.24.0.0/15, 172.26.0.0/15, 172.28.0.0/15, and 172.30.0.0/15.

Calculating the Exhaustion: A /12 network contains exactly eight /15 blocks. By excluding all eight /15 ranges listed in the exhibit, the customer has effectively excluded 100% of the available addresses from the primary 172.16.0.0/12 pool.

Connectivity Problems: When the IPAM pool is exhausted or overly restricted, FortiSASE cannot assign valid, non-overlapping subnets to the PoPs. This leads to connectivity problems for remote users and can cause the system to "fall back" to ranges it believes are available, even if they were intended to be excluded, or simply fail to establish tunnels entirely.

To resolve this, the administrator must ensure that the excluded subnets do not consume the entire pool and that the remaining unexcluded space is large enough to provide a /20 block for every active PoP in their subscription.

Question: 43

Which statement about FortiSASE and SAML is true? (Choose one answer)

A. FortiSASE acts as the SP, relies on an external IdP, and can use SAML group matching.

B. FortiSASE supports SAML login but cannot use SAML group matching.

C. FortiSASE acts as the IdP and can perform SAML group matching internally.

D. FortiSASE includes IdP functionality and uses it for SAML group matching.

Answer: A

Explanation:

FortiSASE utilizes Security Assertion Markup Language (SAML) to provide a seamless Single Sign-On (SSO) experience for remote users connecting to the cloud infrastructure.

Role Identification: In a SAML exchange, FortiSASE functions as the Service Provider (SP). It relies on an external Identity Provider (IdP)—such as Microsoft Entra ID (formerly Azure AD), Okta, or FortiAuthenticator—to authenticate the user's identity and provide security assertions.2

SAML Group Matching: One of the core features of the FortiSASE SAML implementation is the ability to perform group matching. During the authentication process, the IdP sends a SAML assertion that typically includes an "Attribute Statement" containing the user's group memberships.3 FortiSASE captures this attribute and matches it against locally defined SAML user groups.

Policy Enforcement: This group matching capability is critical because it allows administrators to apply different Security Internet Access (SIA) or Secure Private Access (SPA) policies based on the user's role (e.g., "Marketing" vs. "Finance") rather than managing individual users manually.

Analysis of Incorrect Options: * Options C and D are incorrect because FortiSASE does not natively act as a SAML IdP; it is designed to consume assertions from professional identity management platforms.

Option B is incorrect because FortiSASE fully supports and relies upon group matching for enterprise-scale policy management.

Question: 44

What is the purpose of the grace period for off-net endpoints in the FortiSASE Network Lockdown feature? (Choose one answer)

A. To allow users to attempt VPN reconnection before restrictions are applied1

B. To bypass security policies for specific applications

C. To permanently block network access for non-compliant endpoints

D. To automatically reset the FortiClient configuration

Answer: A

Explanation:

In the FortiSASE architecture, Network Lockdown is a security feature designed to prevent off-net (off-fabric) endpoints from accessing the internet or local network without the protection of the SASE security stack.

Triggering Lockdown: When an endpoint is determined to be "off-net"—meaning it does not satisfy the on-net rule sets defined in its endpoint profile—a timer starts for a configurable grace period.

Function of the Grace Period: During this period, the endpoint maintains full access to the LAN and the internet.4 The specific purpose of this grace period is to provide the user with a window of time to attempt a connection to the FortiSASE VPN tunnel or an alternate corporate tunnel.5 This ensures that users can authenticate and regain a secure "on-net" status before any connectivity restrictions are enforced.

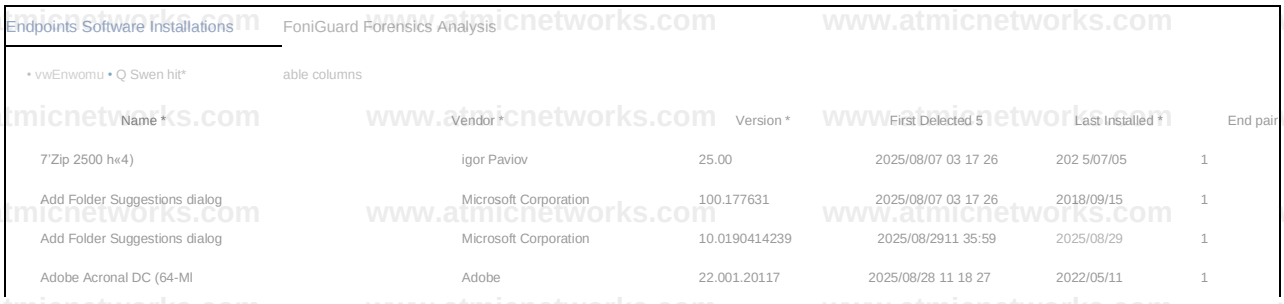
Enforcement: If the grace period expires and the endpoint has failed to establish a VPN connection, FortiClient enforces a strict lockdown.7 In this state, the device cannot reach the LAN or the internet, except for specifically defined "Exempt Destinations" (such as captive portal login pages or the FortiSASE portal itself).

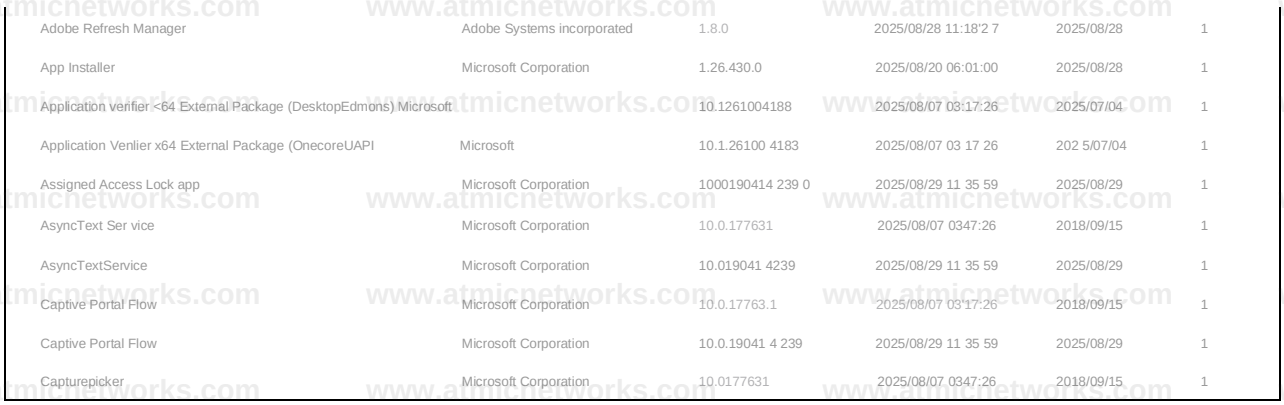
Resetting the Timer: Any attempt to connect to the tunnel during the grace period resets the timer, providing additional opportunities for the user to remediate their connection status.8

According to the FortiSASE 25 Administrator Study Guide, the grace period is an essential userexperience setting that balances strict "zero-trust" security with the practical need for users to access the network briefly to establish their secure tunnel.

Question: 45

Refer to the exhibit.





Adobe Refresh Manager	Adobe Systems incorporated	1.8.0	2025/08/28 11:18'2 7	2025/08/28	1
App Installer	Microsoft Corporation	1.26.430.0	2025/08/20 06:01:00	2025/08/28	1
Application verifier <64 External Package (DesktopEdmons) Microsoft		10.1261004188	2025/08/07 03:17:26	2025/07/04	1
Application Venlier x64 External Package (OnecoreUAPI	Microsoft	10.1.26100 4183	2025/08/07 03 17 26	202 5/07/04	1
Assigned Access Lock app	Microsoft Corporation	1000190414 239 0	2025/08/29 11 35 59	2025/08/29	1
AsyncText Ser vice	Microsoft Corporation	10.0.177631	2025/08/07 0347:26	2018/09/15	1
AsyncTextService	Microsoft Corporation	10.019041 4239	2025/08/29 11 35 59	2025/08/29	1
Captive Portal Flow	Microsoft Corporation	10.0.17763.1	2025/08/07 03'17:26	2018/09/15	1
Captive Portal Flow	Microsoft Corporation	10.0.19041 4 239	2025/08/29 11 35 59	2025/08/29	1
Capturepicker	Microsoft Corporation	10.0177631	2025/08/07 0347:26	2018/09/15	1

Which type of information or actions are available to a FortiSASE administrator from the following output? (Choose one answer)

A. Administrators can view and configure endpoint profiles and ZTNA tags.

B. Administrators can view and configure automatic patching of endpoints, and first detected date for applications.

C. Administrators can view latest application version available and push updates to managed endpoints.

D. Administrators can view application details, such as vendor, version, and installation dates to identify unwanted or outdated software.

Answer: D

Explanation:

The provided exhibit (image_57e69d.jpg) displays the Software Installations dashboard within the FortiSASE portal. This dashboard is a key component of the endpoint visibility and management features provided by the integrated FortiClient EMS functionality.

Visible Metadata: The output provides a granular list of all software detected on managed endpoints, including the application Name, the Vendor (e.g., Igor Pavlov, Microsoft Corporation, Adobe), the specific Version currently installed, and critical timestamps such as First Detected and Last Installed.

Administrative Utility: This information allows an administrator to audit the software environment effectively. By reviewing these details, they can identify unwanted software (PUA), shadow IT, or outdated software versions that may possess known vulnerabilities.

Actions Available: While the primary view is informational, the presence of the View Endpoints button (visible in the top-left) allows administrators to pivot from a specific application to a list of all individual devices where that software is present, facilitating targeted remediation.

Analysis of Incorrect Options:

Option A: While FortiSASE manages profiles and tags, this specific "Software Installations" view is focused purely on software inventory.

Option B: Although the "First Detected" date is visible, FortiSASE does not support "automatic patching" of third-party software directly from this inventory screen.

Option C: The dashboard shows what is installed, not the "latest available" version in the market, nor does it provide a mechanism to "push updates" to these third-party applications.

Question: 46

Which two statements about the Hub Selection Method in FortiSASE Secure Private Access (SPA) are correct? (Choose two answers)

A. When using Hub Health and Priority, FortiSASE selects the highest priority hub that meets the configured SLA thresholds.

B. When using BGP MED, FortiSASE selects the hub with the lowest MED value only if it also meets the configured SLA thresholds.

C. When using SLA thresholds, administrators can customize latency, jitter, and packet loss for each security POP.

D. When using Hub Health and Priority, all hubs with the same priority are always selected regardless of SLA results.

Answer: A, B

Explanation:

According to the NSE7 SASE Enterprise Guide (Pages 64 & 153), FortiSASE utilizes an intelligent engine to manage connectivity to private resources through various selection methods:

Hub Health and Priority: FortiSASE incorporates a built-in SD-WAN engine for intelligent routing selection among established IPsec links. The health check IP address periodically receives performance metrics, including jitter, latency, and packet loss, for each service connection. In this mode, FortiSASE evaluates the available hubs and selects the one with the highest priority (the most preferred value) within each POP, provided that the hub meets the defined service-

level agreement (SLA) requirements. For this configuration to function correctly, both FortiSASE and the SPA hub must use the same Autonomous System Number (ASN).

BGP Multiple Exit Discriminator (MED): This method leverages the standard BGP MED attribute, which allows an autonomous system to signal its preferred entry point to a peer. FortiSASE learns the MED values advertised by the configured hubs. The architecture is designed so that the lower the MED value, the more preferred the path is to the receiving router. Consistent with the "Zero Trust" and "Secure Access" principles, even when using BGP MED, the selection is gated by the health engine; therefore, the hub is only selected if it also satisfies the configured SLA thresholds.

While SLA thresholds can be configured, the primary logic for hub selection focuses on how priority and dynamic routing attributes (like MED) interact with the real-time health of the tunnel.

Question: 47

Which two statements about FortiSASE Geofencing with regional compliance are true? (Choose two answers)

A. You can configure regional compliance on the security POP or the on-premises device, not both.1

B. If no regional compliance rule is configured, the connection is made to the closest security POP.

C. A regional compliance rule can connect only to an on-premises device or only to a security POP.2

D. The connection order for a regional compliance rule is always the security POP first, followed by the on-premises device.

Answer: B, C

Explanation:

FortiSASE Geofencing and Regional Compliance allow administrators to control where remote users connect based on their physical location, which is determined by the endpoint's public IP address.3

Default Connection Behavior: By default, FortiSASE uses a "best-effort" geolocation logic to ensure the lowest latency for the user. If an administrator has not configured a specific regional compliance rule for a user's country or region, FortiClient will automatically attempt to connect to the closest available FortiSASE security PoP (Point of Presence) based on proximity.4

Regional Compliance Rules: When an organization must enforce data residency or specific security routing

requirements, they create Regional Compliance rules. According to the FortiSASE 25 Feature Administration Guide, these rules allow the administrator to override the default "closest PoP" behavior for specific countries.

Connectivity Options: Within a regional compliance rule, the administrator must specify the destination for the traffic. The system provides a choice between two distinct connection types: a FortiSASE Security PoP or an On-premises device (such as a FortiGate acting as a gateway).5 The documentation specifies that a rule is designed to point to one of these types at a time to satisfy the compliance requirement for that specific region.

Connection Priority: While multiple connections can be managed in a priority table, the logic for Regional Compliance is focused on directing the user to the designated compliant entry point. Option D is incorrect because the connection order is determined by the Priority and custom fail-over connections table; an administrator can manually adjust the sequence, so it is not "always" the security PoP first.

Question: 48

What is required to enable the MSSP feature on FortiSASE? (Choose one answer)

A. Multi-tenancy must be enabled on the FortiSASE portal.
B. MSSP user accounts and permissions must be configured on the FortiSASE portal.
C. The MSSP add-on license must be applied to FortiSASE.
D. Role-based access control (RBAC) must be assigned to identity and access management (IAM) users using the FortiCloud IAM portal.

Answer: D

Explanation:

To enable the Managed Security Service Provider (MSSP) feature on FortiSASE, the administrative framework must be established outside of the local SASE instance within the broader FortiCloud ecosystem.

FortiCloud IAM Integration: The FortiSASE MSSP portal relies on FortiCloud Identity & Access Management (IAM) to define the scope of management for internal teams. Administrators do not create local "MSSP users" within the SASE portal itself; instead, they must use the FortiCloud IAM portal to assign specific Role-Based Access Control (RBAC) to IAM users.

Permissions and Scope: These RBAC settings determine which customer tenants (Organizational Units or OUs) an MSSP administrator can view, configure, or monitor. Without the proper role assignment in the IAM portal, the MSSP portal

and its multi-tenant viewing capabilities will not be accessible to the user, even if the account has the necessary licenses.

Hierarchical Management: Once RBAC is correctly assigned, the MSSP administrator can leverage the FortiCloud Organizations service to manage multiple customer accounts from a single pane of glass. This centralized approach ensures that security policies and configurations can be standardized across the entire customer base while maintaining strict data isolation between tenants.

According to the FortiSASE 25 Multitenant Deployment Guide, configuring the IAM portal is the primary prerequisite that grants an MSSP internal team the permissions necessary to perform operations on customer FortiSASE tenants.

Question: 49

You are configuring FortiSASE SSL deep inspection. What is required for FortiSASE to inspect encrypted traffic? (Choose one answer)

A. FortiSASE uses a third-party CA certificate without importing it to client machines, and SSL deep inspection supports only web filtering and application control.

B. FortiSASE acts as a root CA without needing a certificate, and SSL deep inspection is used only for split DNS and video filtering.

C. FortiSASE requires an external CA to issue certificates to client machines, and SSL deep inspection supports only antivirus and file filter.

D. FortiSASE acts as a certificate authority (CA) with a self-signed or internal CA certificate, requiring the root CA certificate to be imported into client machines.

Answer: D

Explanation:

SSL deep inspection (DPI) is a critical security function that allows FortiSASE to decrypt and inspect the actual payload of encrypted traffic (such as HTTPS, SMTPS, and FTPS) to identify and block hidden threats.

The Role of the CA: For this process to occur, FortiSASE must act as a "man-in-the-middle" by intercepting the SSL session, decrypting it for inspection, and then re-encrypting it before sending it to the endpoint.2 To re-encrypt the

traffic, FortiSASE acts as a Certificate Authority (CA) and signs a new certificate for the destination website on the fly.

Certificate Types: This CA role can be fulfilled using the default self-signed certificate provided by Fortinet (typically Fortinet_CA_SSL) or a certificate issued by an organization's internal/private CA. Publicly trusted third-party CAs (like DigiCert or Let's Encrypt) do not sell CA-capable certificates that can be used for this type of inspection.

Client Machine Requirement: Because the endpoint's browser or operating system will not natively trust a certificate signed by a private or self-signed CA, the root CA certificate must be imported into the Trusted Root Certification Authorities store on all managed client machines. Failure to do so results in persistent certificate warnings or blocked connections for the end user.

Supported Features: Once enabled, SSL deep inspection provides the necessary visibility for high- level security features to function, including Antivirus, Web Filtering, Data Loss Prevention (DLP), File Filter, and Application Control.

Question: 50

Which service is included in a secure access service edge (SASE) solution, but not in a security service edge (SSE) solution? (Choose one answer)

A. SWG

B. SD-WAN1

C. CASB

D. ZTNA

Answer: B

Explanation:

The distinction between SASE (Secure Access Service Edge) and SSE (Security Service Edge) is a fundamental architectural concept in modern networking and security.

SASE Definition: SASE is a comprehensive framework that converges networking capabilities (specifically SD-WAN) with cloud-native security services (SSE) into a single, unified service model.

SSE Definition: SSE represents the security-focused subset of SASE.4 It encompasses the core security pillars required for secure access, including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Zero Trust

Network Access (ZTNA).

The Key Differentiator: While both solutions share the same security stack (SWG, CASB, ZTNA), SD- WAN (Software-Defined Wide Area Network) is the specific networking component that exists in a full SASE solution to provide intelligent path selection and optimized connectivity. SSE intentionally excludes these wide-area networking functions, focusing purely on the security service delivery layer.

According to the FortiSASE 25 Enterprise Administrator Study Guide, organizations that already have a robust networking infrastructure and only require a cloud-delivered security overlay would opt for SSE, whereas those seeking a complete transformation of both network and security would deploy a full SASE solution that includes SD-WAN.

Question: 51

How does FortiSASE address the market trends of multicloud and Software-as-a-Service (SaaS) adoption, hybrid workforce, and zero trust? (Choose one answer)

A. It focuses solely on securing on-premises networks, ignoring cloud and remote work challenges.

B. It prioritizes legacy VPN connections for hybrid workforces, bypassing modern cloud and zero-trust security measures.

C. It provides visibility and control for multicloud and SaaS environments, ensures secure and seamless access for hybrid workforces, and implements zero-trust principles.1

D. It supports only zero-trust frameworks without addressing multicloud or hybrid workforce needs.

Answer: C

Explanation:

FortiSASE is designed as a unified, single-vendor solution that specifically targets the convergence of networking and security to address the modern challenges of a distributed enterprise.2

Multicloud and SaaS Adoption: FortiSASE addresses the surge in cloud-first strategies by providing Next-Generation Dual-Mode CASB (Cloud Access Security Broker).3 This feature uses both inline and API-based inspection to provide comprehensive visibility into sanctioned and unsanctioned SaaS applications (Shadow IT), ensuring that data is protected regardless of whether it resides in AWS, Azure, Google Cloud, or SaaS platforms like Microsoft 365.

Hybrid Workforce: To support a workforce that moves between the home, the office, and public spaces, FortiSASE delivers consistent security posture.5 It replaces the inconsistent experience of legacy VPNs with a geographically dispersed network of over 150 Points of Presence (PoPs), ensuring low-latency access to applications while maintaining high-performance SSL inspection and threat detection for all remote users.

Zero Trust Integration: Central to the FortiSASE architecture is Universal ZTNA (Zero Trust Network Access).7 Unlike traditional VPNs that grant broad network access, ZTNA applies the principle of "never trust, always verify". It grants access on a per-session, per-application basis, continuously verifying the device posture and user identity before and during application access.9 This shift from implicit to explicit trust significantly reduces the internal attack surface and mitigates the risk of lateral movement by attackers.

By integrating these components into a single operating system (FortiOS) and managed via a single console, FortiSASE simplifies IT operations while delivering the visibility and control required for today's multicloud and hybrid environments.

Question: 52

A FortiSASE customer has been enforcing always-on VPN for their remote users running FortiClient. What option can be enabled under the customer's Endpoint Profile to allow them access different resources located in the same L2 network? (Choose one answer)

A. Allow local LAN Access in the user Endpoint Profile before they get connected to the VPN

B. Endpoint Sandbox protection for VPN users

C. Endpoint Anti-Virus protection in the Endpoint Profile for VPN

D. Network Lockdown for endpoints with VPN enabled

Answer: A

Explanation:

In a FortiSASE environment where always-on VPN is enforced, FortiClient typically establishes a full tunnel to a Security Point of Presence (PoP). By default, a full-tunnel configuration instructs the endpoint to send all traffic—including traffic destined for the local network—through the secure tunnel to FortiSASE for inspection.

The Local Access Challenge: When a remote user is at home or in a satellite office, they often need to access local resources such as printers, NAS devices, or other computers on the same Layer 2 (L2) broadcast domain. In a standard

full-tunnel setup, these local resources become unreachable because the routing table on the endpoint prioritizes the VPN interface for all non-local-gateway traffic.

Allow Local LAN Access: To resolve this while maintaining the security of the "Always-On" requirement, FortiSASE administrators can enable the Allow Local LAN Access feature within the Endpoint Profile.

Configuration Logic: This setting modifies the FortiClient configuration (often via an XML update

pushed from the FortiSASE EMS) to include an exemption for the endpoint's locally connected subnet. Specifically, it ensures that traffic destined for the local L2 network does not enter the IPsec or SSL-VPN tunnel, allowing the user to interact with local peripherals while all other internet and corporate-bound traffic remains secured by FortiSASE.

Incorrect Options: * Option B and C: Sandbox and Anti-Virus protections are security features for threat detection and do not influence the routing of local network traffic.

Option D: Network Lockdown actually does the opposite; it restricts network access until a VPN connection is established and typically blocks local LAN access unless specific exemptions are made, making it the incorrect choice for enabling access to local resources.

Question: 53

Which three traffic flows are supported by FortiSASE Secure Private Access (SPA)? (Choose three answers)

A. From private resources to FortiSASE agent-based users.

B. From private resources to the internet.

C. From agent-based users to private resources behind the Fortinet SD-WAN.

D. From private resources to other private resources (SPA to SPA).

E. From thin branches/branch on-ramp to private resources behind the Fortinet SD-WAN.

Answer: A, C, E

Explanation:

FortiSASE Secure Private Access (SPA) provides flexible connectivity to internal corporate resources using a hub-and-

spoke architecture where FortiSASE PoPs act as spokes to an organization's FortiGate hub.

Flow from Agent-based users to Private Resources (C): This is the core functionality of SPA. Remote users running FortiClient (agent-based) connect to the nearest FortiSASE PoP. The PoP, integrated into the corporate SD-WAN fabric, uses IPsec and BGP to route traffic to the private applications

located behind the FortiGate hub or associated spokes.

Flow from Thin Branches/Branch On-ramp to Private Resources (E): FortiSASE extends its security and connectivity to physical locations through "Thin Edge" (e.g., FortiExtender, FortiAP) or "Branch On- ramp" (e.g., branch FortiGates). These sites form tunnels to the FortiSASE PoP, which then provides them with access to the same private resources in the SD-WAN network as the remote agent-based users.

Flow from Private Resources to Agent-based users (A): The SPA architecture is designed for bidirectional communication. Documentation confirms that traffic can be initiated from the FortiGate hub (or local networks behind it) to the remote VPN agents. This "Server-to-Client" flow is essential for administrative tasks, log forwarding, or real-time communication applications like VoIP.

Incorrect Options:

Option B: Traffic from private resources to the internet is handled via Secure Internet Access (SIA) or local gateway policies, not the SPA use case, which is dedicated to internal private application access.

Option D: While FortiSASE can facilitate branch-to-branch communication via ADVPN shortcuts, the term "SPA" specifically refers to the access layer for users and is not used to describe resource-to- resource or hub-to-hub traffic.

Question: 54

You have configured FortiSASE Secure Private Access (SPA) deployment. Which statement is true about traffic flows? (Choose two answers)

A. When using SD-WAN private access, traffic goes from an endpoint directly to an SPA hub.

B. When using zero trust network access, traffic goes from an endpoint to a FortiSASE POP, and then to a ZTNA access proxy.

C. When using zero trust network access (ZTNA) traffic goes from an endpoint directly to a ZTNA access proxy.

D. When using SD-WAN private access, traffic goes from an endpoint to a FortiSASE POP, and then to an SPA hub.

Answer: C, D

Explanation:

FortiSASE Secure Private Access (SPA) offers two distinct architectural methods for connecting remote users to private applications: SD-WAN-based SPA and ZTNA-based SPA. Each utilizes a different traffic flow to balance security and performance requirements.

SD-WAN Private Access (Hub-and-Spoke): In this model, the FortiSASE Security Points of Presence (PoPs) act as spokes in a traditional hub-and-spoke VPN topology. When a remote user attempts to access a private network, the traffic is first steered to the closest FortiSASE PoP. The PoP then routes that traffic over a persistent IPsec tunnel to the corporate FortiGate hub (or SPA hub). This ensures that all traffic, regardless of protocol (TCP/UDP), can be inspected by the SASE security stack before entering the private network.

Zero Trust Network Access (ZTNA): Unlike the SD-WAN approach, ZTNA is designed for a "shortest path" connection. While FortiSASE manages the endpoint's posture and issues certificates, the actual application traffic (the data plane) bypasses the FortiSASE PoP. Instead, the FortiClient agent on the endpoint establishes a direct HTTPS or TCP-forwarding connection to the ZTNA Access Proxy configured on the corporate FortiGate. This significantly reduces latency and is ideal for high- performance TCP-based applications.

According to the FortiSASE 25 Secure Internet Access Architecture Guide, "In FortiSASE, ZTNA refers to traffic that is destined directly to private resources using the FortiGate ZTNA access proxy traffic flow," whereas for SD-WAN SPA, the PoPs "rely on IPsec overlays... to secure and route traffic between PoPs and the networks behind an organization's SD-WAN hubs."

Question: 55

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. How can you provide secure internet access to the contractor using FortiSASE? (Choose one answer)

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

B. Use a tunnel policy with a contractors user group as the source on FortiSASE to provide internet access.

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

D. Use the self-registration portal on FortiSASE to grant internet access.

Answer: A

Explanation:

In the FortiSASE architecture, there are two primary methods for delivering Secure Internet Access (SIA): Agent-based (using FortiClient) and Agentless (using Secure Web Gateway/SWG).

Use Case Analysis: The scenario describes a contractor—an unmanaged user—who requires temporary access for a web-based application (the POS system). For contractors or guests using personal/non-corporate devices where installing the FortiClient agent is either not feasible or not desired, FortiSASE provides the SIA Agentless deployment model.

Mechanism (SWG & PAC): In this mode, FortiSASE functions as an explicit web proxy. To steer the contractor's web traffic (HTTP/HTTPS) to the SASE cloud for inspection, the administrator provides the user with a proxy auto-configuration (PAC) file. The contractor simply configures their browser or operating system to point to the URL of this PAC file.

Security Enforcement: Once the PAC file is applied, all web traffic from the contractor's device is redirected to the FortiSASE SWG PoP. Here, the traffic is subject to the organization's full security stack, including SSL deep inspection, Antivirus, Web Filtering, and Application Control, ensuring that even temporary contractor access is fully secured and logged.

Why other options are incorrect:

Option B (Tunnel Policy): This refers to agent-based access where a VPN tunnel is established. This requires FortiClient, which is generally not used for temporary contractors on unmanaged devices.

Option C (ZTNA Unmanaged): While ZTNA supports agentless access to private applications (SPA), providing internet access (SIA) to an unmanaged endpoint is specifically the role of the SWG/Proxy service.

Option D (Self-registration): While FortiSASE has a User Portal for onboarding, it is a method for user registration/credential management, not the technical traffic-steering mechanism used to provide internet connectivity.

According to the FortiSASE 25 Secure Internet Access Architecture Guide, the SWG (Agentless) approach is the recommended best practice for securing web-only traffic from unmanaged endpoints and third-party contractors.

Question: 56

What are two benefits of deploying secure private access (SPA) with SD-WAN? (Choose two answers)

A. ZTNA posture check performed by the hub FortiGate

B. Support of both TCP and UDP applications

C. A direct access proxy tunnel from FortiClient to the on-premises FortiGate

D. Inline security inspection by FortiSASE

Answer: B, D

Explanation:

According to the NSE7 SASE Enterprise Guide (Pages 46 & 61), deploying Secure Private Access (SPA) with SD-WAN provides advanced security and networking capabilities by routing traffic through global Points of Presence (PoPs).

Inline Security Inspection (D): A major advantage of this approach is that traffic is routed through FortiSASE PoPs before it reaches private applications. This enables inline security inspection, providing robust protection against threats by applying the full SASE security stack—including antivirus, intrusion prevention, and deep packet inspection—to private access traffic.

Support for TCP and UDP (B): Organizations with existing FortiGate SD-WAN deployments benefit from broader and seamless access to privately hosted applications. The SD-WAN SPA use case explicitly supports both TCP- and UDP-based applications, ensuring that legacy or specialized services that rely on UDP function correctly over the secure tunnel.

SD-WAN Optimization: This method leverages the benefits of SD-WAN to optimize traffic flow between the SASE PoP and the corporate SD-WAN hub or data center FortiGate. It is particularly useful for mission-critical applications that require an extra layer of security combined with path optimization.

Architecture: In this configuration, the FortiSASE Security PoPs act as spokes in the organization's SD- WAN network, relying on IPsec VPN overlays and BGP for secure dynamic routing.

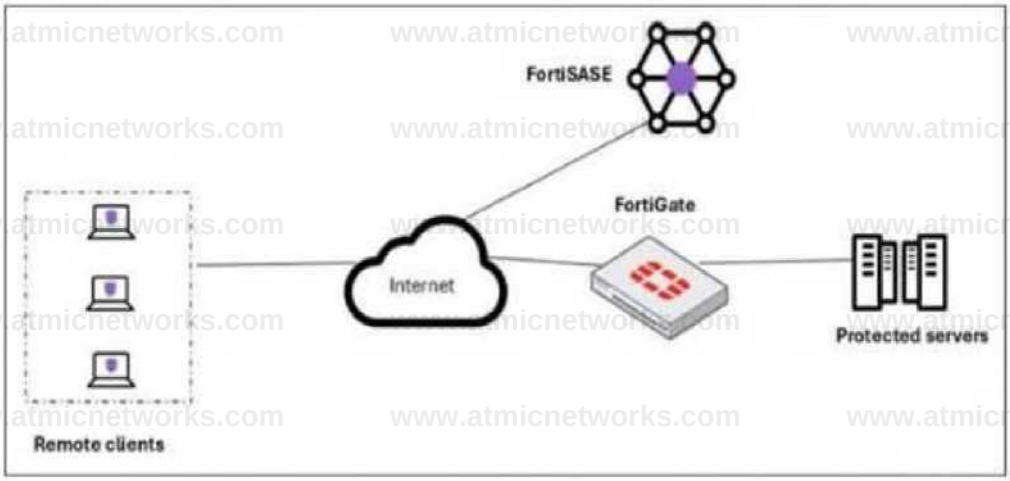
While ZTNA posture checks are a feature of the broader ecosystem, the NSE7 Guide specifically highlights inline inspection and application support (TCP/UDP) as primary advantages of the SD-WAN

integrated SPA approach.

Question: 57

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 two setups will achieve these requirements? (Choose two answers)

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.

Answer: B, C

Explanation:

To implement Zero Trust Network Access (ZTNA) where a FortiGate hub enforces device posture and processes traffic directly, specific architectural and configuration steps are required on the FortiGate appliance.

ZTNA Access Proxy (B): The FortiGate must be configured as a ZTNA access proxy. In this role, the FortiGate acts as a secure gateway that mediates connections between remote users and internal applications. This setup ensures that all TCP traffic is intercepted and processed by the FortiGate, providing a direct, shortest-path connection that bypasses the FortiSASE cloud PoPs for the data plane.

ZTNA Servers and Policies (C): Within the FortiGate configuration, administrators must define ZTNA servers (which identify the protected applications or resources) and ZTNA policies. ZTNA policies are the enforcement rules that check for valid client certificates and specific ZTNA tags (synchronized from FortiSASE) before allowing access to a resource. This configuration allows the FortiGate to perform continuous posture checks on every session.

Posture Check Mechanism: While ZTNA tags are used, they are generally synchronized from the FortiSASE Endpoint Management Service (EMS) rather than manually configured on the FortiGate itself. This synchronization ensures the FortiGate has real-time visibility into the security posture (e.g., AV compliance, OS version) of the endpoints as reported by FortiClient.

Analysis of Incorrect Options:

Option A: Creating ZTNA tags manually on a FortiGate is technically possible but is not the recommended "setup" in a FortiSASE deployment, as tags are meant to be dynamically assigned by EMS and synced to the fabric.

Option D: "Private access policies on FortiSASE" refers to the SD-WAN Secure Private Access (SPA) use case. In the SD-WAN SPA model, traffic is steered through the FortiSASE PoP first, whereas the requirement specifically asks for TCP traffic to be processed by the FortiGate using ZTNA.

Question: 58

Your FortiSASE customer has a small branch office in which ten users will be using their personal laptops and mobile devices to access the internet. Which deployment should they use to secure their internet access with minimal configuration? (Choose one answer)

A. FortiClient endpoint agent to secure internet access

B. FortiAP to secure internet access

C. SD-WAN on-ramp to secure internet access

D. FortiGate as a LAN extension to secure internet access

Answer: B

Explanation:

For small branch offices (thin edges) where users utilize unmanaged personal devices (BYOD) like laptops and mobile phones, the most efficient way to provide Secure Internet Access (SIA) with minimal configuration is by deploying a FortiAP.

Thin Edge Integration: FortiSASE includes expanded integrations with the Fortinet WLAN portfolio, allowing FortiAP wireless access points to function as "thin edge" devices. These access points intelligently ofload and steer traffic from the branch directly to the nearest FortiSASE Security Point of Presence (PoP).

No Endpoint Agents Required: Because the devices are personal and unmanaged, installing the FortiClient agent (Option A) is often not feasible or desirable. The FortiAP deployment secures all client devices at the location without requiring any endpoint agents.

Minimal Configuration & Zero-Touch: This solution is specifically designed for small office locations with limited budgets and no local IT staff. FortiSASE offers cloud-delivered management with zerotouch provisioning for FortiAP. Once the AP is connected, it automatically establishes a secure CAPWAP or IPsec tunnel to FortiSASE, ensuring all connected users are protected by the cloud security stack (Antivirus, Web Filtering, etc.) with almost no manual setup on the end-user side.

Why other options are less ideal:

Option C and D: SD-WAN on-ramp and FortiGate LAN extensions typically require a physical FortiGate appliance at the branch. For a small office with only ten users and personal devices, this adds unnecessary hardware costs and configuration complexity compared to a simple, cloud-managed FortiAP.

Question: 59

An administrator must restrict endpoints from certain countries from connecting to FortiSASE. Which configuration can achieve this? (Choose one answer)

A. A network lockdown policy on the endpoint profiles

B. Source IP anchoring to restrict access from the specified countries

C. A geography address object as the source for a deny policy

D. Geofencing to restrict access from the required countries

Answer: D

Explanation:

To restrict endpoints from certain countries from connecting to FortiSASE, the administrator should configure Geofencing. This feature provides granular control over which geographic locations are permitted or denied access to the SASE infrastructure.

Geofencing in FortiSASE

Geofencing is the primary mechanism for controlling remote user connectivity based on their origin.

Functionality: It uses a geography-to-IP mapping database to identify the location of incoming connection requests.

Access Modes: Administrators can choose between two main modes:

Allow: Only users from specified countries can connect; all others are blocked.

Deny: Users from specified countries are blocked; all others are allowed.

Configuration Path: In the FortiSASE GUI, navigate to Configuration > Geofencing to enable the feature and add the relevant countries.

Enforcement: Once enabled, the system automatically creates "local-in" policies to drop or permit traffic at the edge of the SASE PoPs before it can consume resources or attempt authentication.

Question: 60

Which two settings are automatically pushed from FortiSASE to FortiClient in a new FortiSASE deployment with default settings? (Choose two answers)

A. FortiSASE certificate authority (CA) certificate

B. Tunnel profile

C. Real-time protection

D. Zero trust network access (ZTNA) tags1

Answer: A, B

Explanation:

In a standard FortiSASE agent-based deployment, the FortiSASE Endpoint Management Service (EMS) acts as the central control plane for all managed FortiClient instances. When an endpoint is onboarded, the system is designed to provide "zero-touch" configuration for the core connectivity and security components.

CA Certificate (A): For SSL deep inspection to function without triggering browser certificate warnings, the endpoint must trust the FortiSASE CA. FortiSASE supports automatically installing the FortiSASE CA certificate for managed agent-based users. Once the endpoint connects to the FortiSASE EMS, the service automatically deploys the CA certificate to the trusted certificate store of the client machine.

Tunnel Profile (B): To enable Secure Internet Access (SIA), FortiClient requires a pre-configured VPN or tunnel profile that points to the FortiSASE cloud infrastructure. In a new deployment with default settings, FortiSASE automatically pushes the tunnel profile (including gateway information and autoconnect settings) to the FortiClient endpoint. This allows the user to establish a full-tunnel connection to the nearest Security PoP immediately after onboarding.

Analysis of Incorrect Options:

Real-time protection (C): While FortiSASE can manage Malware Protection and Sandbox settings, specific "Real-time protection" features often require manual activation or specific configuration within the Malware Protection profile before being pushed; they are not necessarily "automatically" active in the absolute default state without a profile assignment.

ZTNA tags (D): ZTNA tags are dynamic security posture attributes. While FortiSASE evaluates the endpoint to determine which tags apply, the tags themselves are not "pushed" to the client as a setting; rather, the ZTNA connection rules are pushed, and the tags are synchronized back to the security fabric for posture enforcement.

Question: 61

What can be configured on FortiSASE as an additional layer of security for FortiClient registration? (Choose one answer)

A. Security posture tags

B. User verification

C. Device identification1

D. Application inventory

Answer: B

Explanation:

In a default FortiSASE deployment, endpoints are typically onboarded using a shared invitation code sent via email. While this code simplifies deployment, it can represent a security risk if the code is leaked or intercepted, as any device with the code could potentially register with the SASE management service.

User Verification (SAML SSO): To mitigate this risk, administrators can enable user verification as an additional layer of security.3 When this feature is enforced, entering the invitation code is no longer sufficient to complete registration.

Authentication Workflow: After the end user enters the invitation code in FortiClient, they are prompted to provide their corporate credentials via a SAML SSO login.5 FortiSASE acts as the Service Provider (SP), while an external identity provider (IdP) such as Microsoft Entra ID, Okta, or FortiAuthenticator verifies the user's identity.

Security Benefit: This ensures that only authenticated users—not just anyone with a valid code—can successfully register an endpoint and receive the organization's security and VPN profiles. It prevents unauthorized "shadow" endpoints from joining the managed environment.

Incorrect Options:

Option A: Security posture tags are used after registration to determine if an endpoint is compliant

(e.g., checking if an antivirus is active); they do not secure the registration process itself.

Option C and D: Device identification and application inventory are monitoring and visibility features that occur once the endpoint is already managed.

Refer to the exhibit. Based on the configuration shown in image_595357.jpg, FortiSASE will process sessions requiring FortiSandbox inspection in the following two ways:

A . Only endpoints assigned a profile for sandbox detection will be processed by the sandbox feature.

C . All files executed on a USB drive will be sent to FortiSandbox for analysis.

Answer: A, C

Explanation:

The provided exhibit displays an Endpoint Profile configuration specifically for the Sandbox module. This profile controls how the FortiClient agent on remote endpoints interacts with the integrated FortiSASE cloud sandbox engine.

Profile Assignment (A): In the FortiSASE architecture, security and endpoint settings are organized into profiles that must be explicitly assigned to users or user groups via endpoint policies.

Consequently, the sandbox detection and remediation features are active only on those endpoints that have been assigned this specific endpoint profile. If an endpoint is not assigned a profile with sandbox enabled, it will not submit files for analysis.

Removable Media Analysis (C): Under the File Submission Options, the toggle for All Files Executed from Removable Media is enabled (shown in blue). Since USB drives are the most common form of removable media, this configuration ensures that any file executed from a USB drive is intercepted by FortiClient and submitted to the FortiSASE sandbox for behavioral analysis before being allowed to run, protecting the endpoint from ofline-delivered threats.

Understanding Verdict Levels (B): The exhibit shows the Action is set to Quarantine and the Sandbox Detection Verdict Level is set to Medium. This configuration functions as a threshold; FortiClient will quarantine any file that receives a

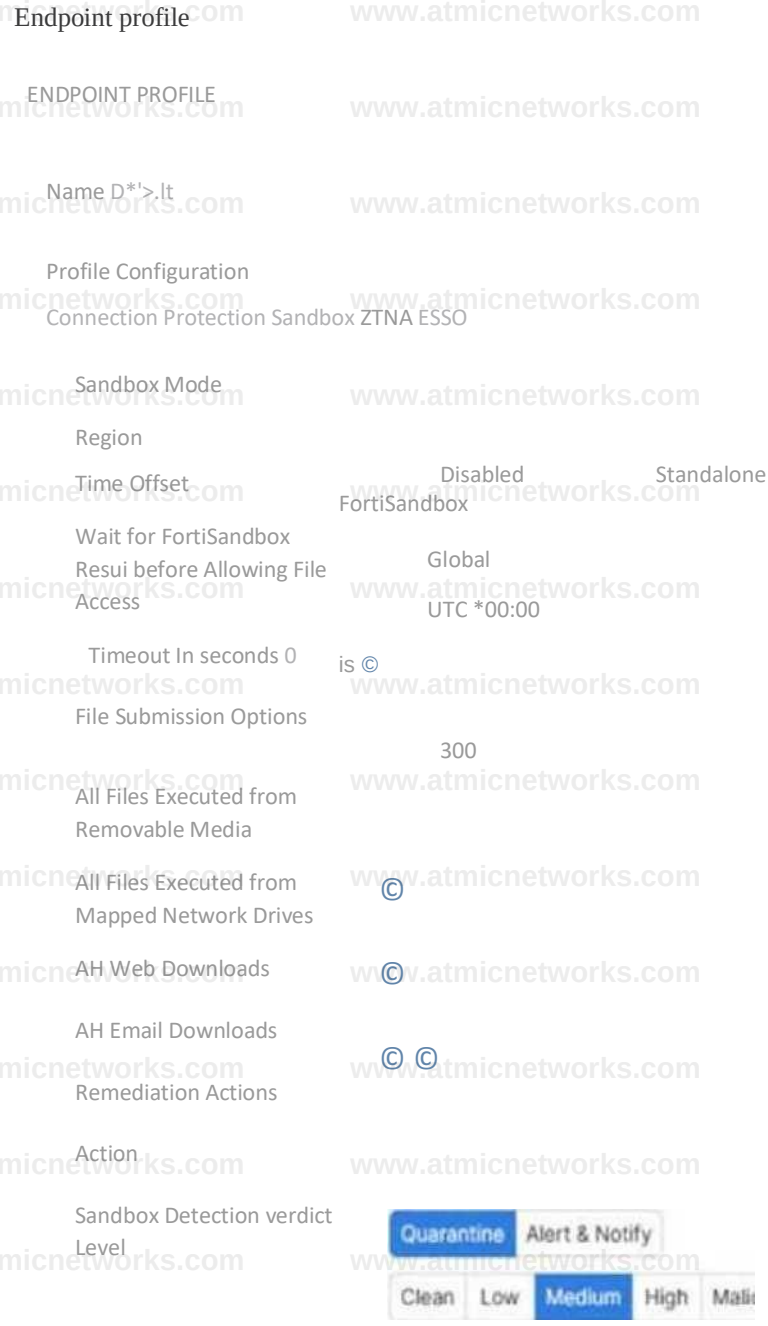
verdict of Medium or higher (including High and Malicious).

Option B is incorrect because it claims only medium-level files are quarantined, which ignores the high-risk and malicious files that would also be blocked.

Sandbox Mode (D): The Sandbox Mode is clearly set to FortiSASE, which utilizes the built-in cloudnative sandbox. This contradicts Option D, which suggests the use of an on-premises or standalone sandbox appliance.

Question: 62

Refer to the exhibit.



Based on the configuration shown, in which two ways will FortiSASE process sessions that require FortiSandbox inspection? (Choose two answers)

A. All files will be sent to an on-premises FortiSandbox for inspection.

B. FortiClient quarantines only infected files that FortiSandbox detects as medium level.

C. All files executed on a USB drive will be sent to FortiSandbox for analysis.

D. Only endpoints assigned a profile for sandbox detection will be processed by the sandbox feature.

Answer: C, D

Explanation:

The exhibit (image_595357.jpg) illustrates the Sandbox configuration tab within a FortiSASE Endpoint Profile. This profile dictates how the managed FortiClient agent handles suspicious files and interacts with the sandbox service.

Profile-Based Enforcement: In the FortiSASE architecture, security features are not applied globally by default; they are enabled through specific profiles assigned to endpoints. Therefore, the sandbox inspection and remediation logic will only be active for endpoints that have been assigned a profile where the Sandbox feature is enabled.

Removable Media Protection: Under the File Submission Options in the exhibit, the setting All Files Executed from Removable Media is toggled on. This ensures that any file executed from a USB drive or other external storage is sent to the FortiSandbox for analysis before being permitted to run on the endpoint.

Sandbox Mode: The Sandbox Mode is set to FortiSASE, indicating that files are sent to the integrated cloud-native sandbox rather than an on-premises appliance. This makes Option A incorrect.

Quarantine Threshold: The Remediation Actions show that the Action is set to Quarantine for files meeting the Sandbox Detection Verdict Level of Medium. This acts as a minimum threshold;
FortiClient will quarantine files identified as Medium, High, or Malicious. Option B is incorrect because it implies only medium-level files are quarantined, whereas higher-risk levels would also be blocked.

Question: 63

Which statement best describes the Digital Experience Monitor (DEM) feature on FortiSASE? (Choose one answer)

A. It monitors the FortiSASE POP health based on ping probes.

B. It is used for performing device compliance checks on endpoints.

C. It provides end-to-end network visibility from all the FortiSASE security PoPs to a specific SaaS application.

D. It gathers all the vulnerability information from all the FortiClient endpoints.

Answer: C

Explanation:

The Digital Experience Monitor (DEM) feature in FortiSASE is a specialized monitoring tool integrated into the SASE cloud to ensure optimal application performance and user satisfaction.2

Purpose and Visibility: DEM is designed to provide end-to-end network visibility by monitoring the health and performance of the connections between the global FortiSASE security Points of Presence (PoPs) and specific SaaS applications (such as Microsoft 365, WebEx, or Dropbox).

Performance Metrics: It identifies and helps troubleshoot issues related to latency, jitter, and packet loss. By leveraging vantage points within the SASE infrastructure, administrators can determine if a performance bottleneck resides within the local network, the SASE backbone, or the SaaS provider's environment.

Integration: This feature is often powered by FortiMonitor, allowing for synthetic transaction monitoring (STM) to simulate user interactions and proactively spot performance issues before they impact the hybrid workforce.

Operational Efficiency: By providing comprehensive insights across users and PoPs, DEM reduces the time required to resolve "slowness" complaints, which are common in remote work scenarios.

Comparison of Other Features:

Option A: While FortiSASE monitors PoP health, DEM's primary value is the end-to-end path to the application.

Option B: Compliance checks are a function of Endpoint Profiles and ZTNA tagging rules, not the monitoring dashboard.

Option D: Vulnerability management is handled by the Vulnerability Scan feature within the managed FortiClient settings.

Question: 64

You are designing a new network, and the cybersecurity policy mandates that all remote users working from home must always be connected and protected. Which FortiSASE component facilitates this always-on security measure? (Choose one answer)

A. Unified FortiClient

B. SDWAN on-ramp2

C. Secure web gateway

D. Thin-branch SASE extension

Answer: A

Explanation:

In a FortiSASE environment, the Unified FortiClient agent is the critical component that fulfills the requirement for "always-on" connectivity and security for remote users.

Persistent Encrypted Tunnels: The Unified FortiClient maintains a persistent, always-on connection to the FortiSASE infrastructure.4 This is typically achieved through an auto-connect VPN tunnel (SSL or IPsec) that initiates as soon as the user logs into their device and has internet access.

Continuous Security Enforcement: By staying connected to a nearby FortiSASE Point of Presence (PoP), the endpoint ensures that all traffic is inspected. This allows the organization to enforce a consistent security posture—including Web Filtering, Antivirus, and Application Control—regardless of whether the user is at home, in a coffee shop, or traveling.

Zero-Trust Integration: Beyond simple connectivity, the unified agent supports Universal ZTNA. It continuously verifies the identity of the user and the security posture of the device before granting access to specific applications, thereby satisfying modern zero-trust security mandates.

Comparison of Other Components:

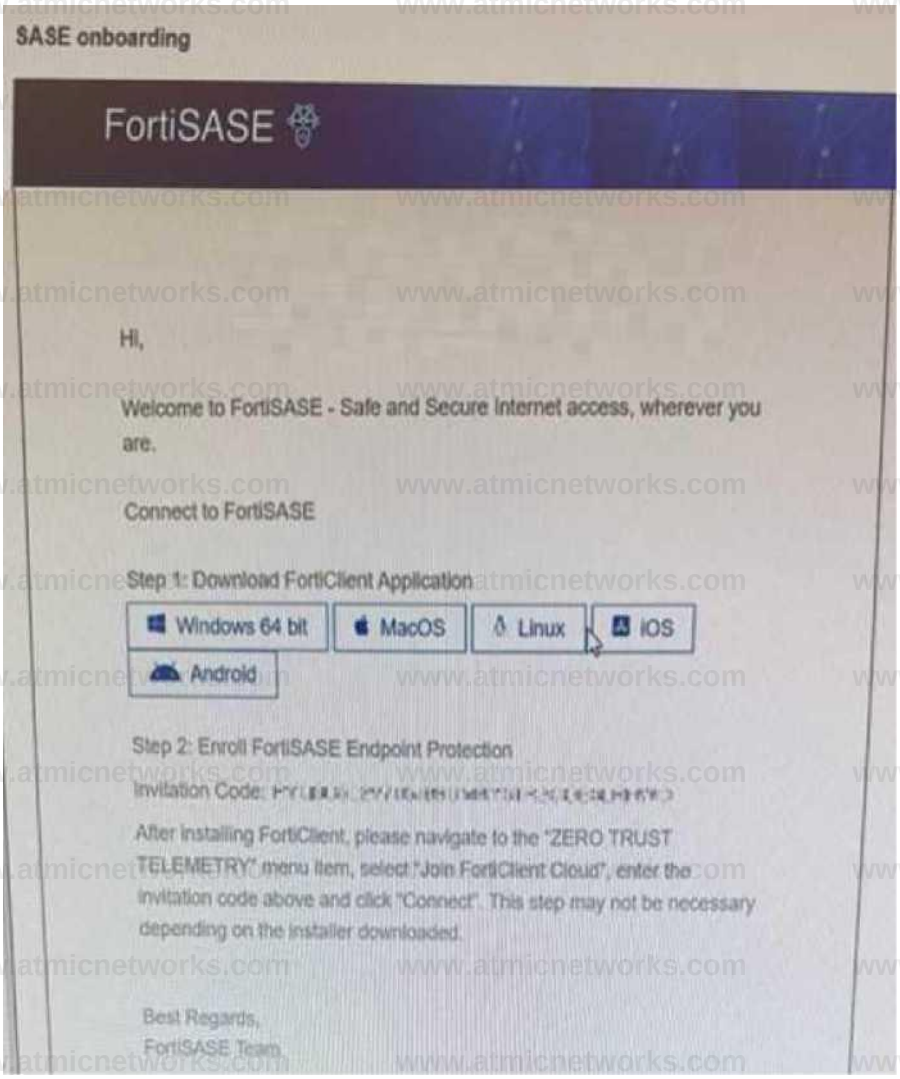
SD-WAN on-ramp (B): Used primarily to integrate existing branch office SD-WAN networks with the SASE cloud for private application access.

Secure Web Gateway (C): While a feature of the SASE PoP, the agentless SWG deployment (using PAC files) does not provide the same level of "always-on" persistent tunnel protection as the FortiClient agent.

Thin-branch SASE extension (D): Focused on securing small branch locations (using FortiAP or FortiExtender) where individual client agents may not be deployed on every device.

Question: 65

Refer to the exhibit.



Which two statements about the onboarding process shown in the exhibit are true? (Choose two answers)

A. The user must manually select which FortiSASE components to install during the FortiClient setup.

B. Depending on the installer used, the invitation code step may be skipped.

C. The invitation code must always be entered manually after installing FortiClient.

D. This is an email from the FortiSASE platform to an end user.

Answer: B, D

Explanation:

The exhibit (image_6361c9.jpg) displays a standard SASE onboarding email sent from the FortiSASE platform to an

end user to facilitate the enrollment of their device.

Communication Source (D): This email is generated by the FortiSASE administrator through the Onboard Users menu in the FortiSASE portal. It provides the user with direct download links for the FortiClient application and a unique Invitation Code required for telemetry connection.

Installer Types and Automation (B): FortiSASE provides two primary methods for deploying the client agent:
Pre-configured Installer: This version is pre-packaged with the organization's unique invitation code built-in. When a user runs this installer, the invitation code step is skipped as the client automatically registers to the correct FortiSASE instance upon installation.

Manual Installer: This version requires the user to manually copy and paste the invitation code from the onboarding email into the FortiClient "Zero Trust Telemetry" menu to complete enrollment.
Analysis of Incorrect Options:

Option A: FortiSASE utilizes a unified agent (FortiClient). The components (VPN, ZTNA, Web Filter, etc.) are managed via Endpoint Profiles assigned in the SASE portal and pushed to the client automatically; they are not manually selected by the user during installation.

Option C: As noted above, if the administrator provides a pre-configured installer, the manual entry of the code is not required, making the statement that it must "always" be entered manually false.

Question: 66

What are the two key features and benefits of Fortinet SOCaaS when integrated with FortiSASE? (Choose two answers)

A. Fortinet SOCaaS offers monitoring only during standard business hours, uses AI without human analysis, and provides annual reports without dashboards or FortiSASE integration.

B. Fortinet SOCaaS monitors only remote users, does not support log forwarding, and provides threat notifications without response guidance or expert meetings.

C. Fortinet SOCaaS allows for consistent security monitoring through log forwarding, offers rapid threat notifications and response guidance, and includes intuitive dashboards.

D. Fortinet SOCaaS provides 24x7x365 cloud-based monitoring by Fortinet experts using AI, machine learning, and human analysis.

E. Fortinet SOCaaS is a standalone service that monitors only FortiGate environments, provides automated patching without human analysis, and does not integrate with FortiSASE.

Answer: C, D

Explanation:

Integrating Fortinet SOCaaS (Security Operations Center as a Service) with FortiSASE provides a managed extension of your security team, combining automated AI/ML-driven triage with human expertise to secure remote and on-premises users.

Consistent Security Monitoring and Dashboards (C): Fortinet SOCaaS ensures that your security posture remains robust through seamless integration. This is achieved by configuring FortiSASE to forward pertinent security logs to the SOCaaS cloud, ensuring that analysts have the necessary data to detect anomalies across your network. The service provides verified threat notifications with detailed response guidance and mitigation recommendations. Furthermore, a built-in portal offers intuitive dashboards to track threats and manage escalated alerts.

24x7x365 Expert-Led Monitoring (D): This feature addresses the cybersecurity skills gap by providing around-the-clock vigilance. A global team of Fortinet Security Analysts works 24x7x365 to monitor

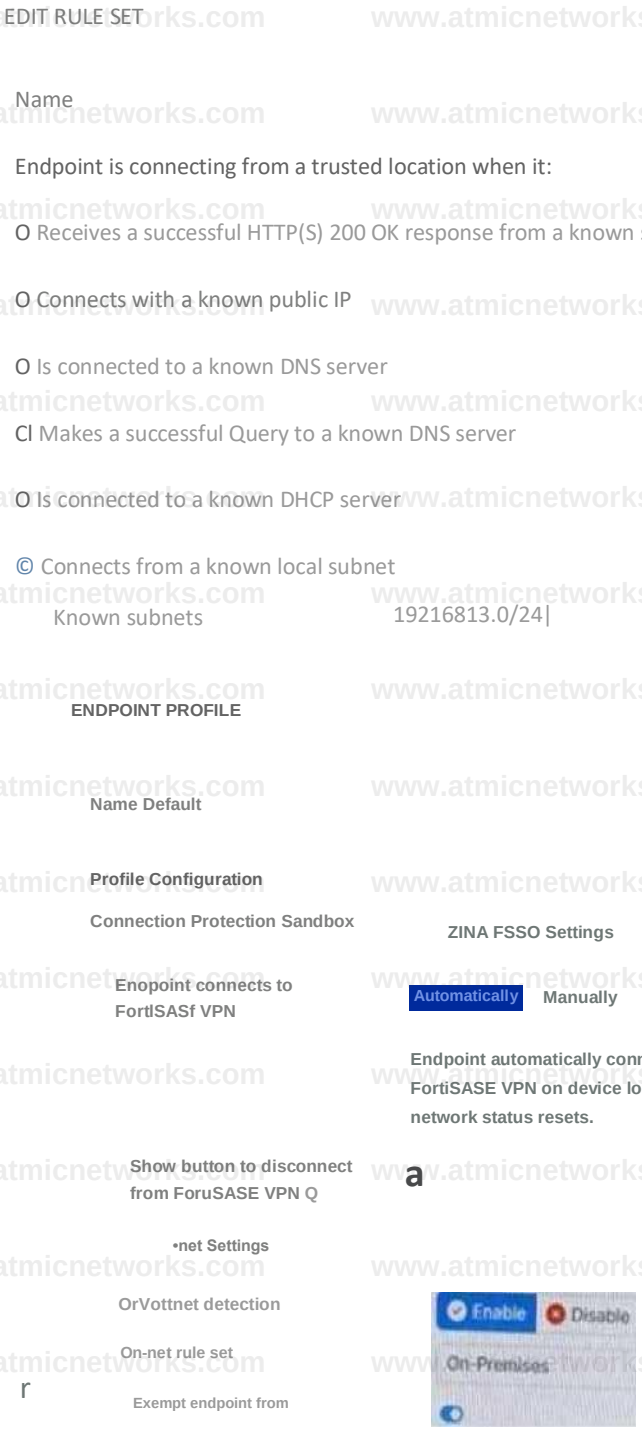
logs and investigate events. The platform leverages AI and Machine Learning for automated alert triage, while human experts perform in-depth analysis to eliminate false positives and validate threats.

Operational Efficiency: By ofloading tedious manual work and triage to Fortinet experts, your internal security team can reduce burnout and focus on higher-value tasks while maintaining a superior security posture for both SASE and on-premises environments.

Question: 67

Refer to the exhibits.

On-net rule set



An endpoint is assigned an IP address of 192.168.13.101/24. Which action will be run on the endpoint? (Choose one answer)

A. The endpoint will be able to bypass the on-net rule because it is connecting from a known subnet.
B. The endpoint will be detected as off-net.
C. The endpoint will be exempted from auto-connect to the FortiSASE tunnel.
D. The endpoint will automatically connect to the FortiSASE tunnel.

Answer: C

Explanation:

Based on the provided exhibits and the logic of FortiSASE On/off-net detection, the endpoint's behavior is determined by its network environment relative to the configured rules.

Subnet Matching and Detection: The On-net rule set (named "On-Premises") is configured to identify a trusted location when the endpoint "Connects from a known local subnet". The administrator has defined the known subnet as $192.168.13.0/24$. Since the endpoint's IP address is $192.168.13.101$, it falls within this range. Consequently, FortiClient detects the endpoint as being on-net (on-fabric).

Action Logic (Exemption): In a FortiSASE Endpoint Profile, when On/off-net detection is enabled and an endpoint matches an "On-net" rule, the standard behavior is to exempt the endpoint from autoconnecting to the FortiSASE VPN tunnel. This design assumes the endpoint is already in a secured office environment where the corporate firewall (FortiGate) provides the necessary protection, making the SASE tunnel redundant.

Comparison of Other Options: * Option B: Incorrect, because the IP matches the defined "known local subnet" rule for on-net detection.

Option D: Incorrect, as auto-connect only triggers when the endpoint is detected as off-net to ensure remote security.

Question: 68

Which two benefits come from integrating SoCaaS with FortiSASE? (Choose two answers)

A. Eliminates the need of endpoint projection software

B. Continuous threat monitoring of all connected endpoints

C. Centralized visibility of all threat events

D. Provides bandwidth usage analytics

Answer: B, C

Explanation:

The integration of FortiGuard SOCaaS with FortiSASE significantly strengthens an organization's security posture by ofloading complex security operations to Fortinet's expert analysts.4

Continuous Threat Monitoring (B): FortiGuard SOCaaS provides 24x7x365 threat monitoring for all endpoints connected to the FortiSASE environment. This service eliminates the need for organizations to hire and maintain their own round-the-clock security operations staff while ensuring that threats are detected and verified in as little as 15 minutes.

Centralized Visibility (C): By forwarding FortiSASE logs to the SOCaaS cloud, administrators gain centralized visibility of all security events through a single, user-friendly portal. This portal allows security teams to track threats, review expert-led incident escalations, and communicate directly with Fortinet SOC analysts to streamline the incident response process.

Operational Efficiency: The integration uses AI-driven alert triage and automated correlation to distill data from the Fortinet Security Fabric, focusing on legitimate threats and reducing the alert fatigue often experienced by internal IT teams.

Question: 69

What are the key differences between the FortiSASE BGP per overlay and BGP on loopback routing design methods? (Choose one answer)

A. BGP per overlay can use separate iBGP sessions for each spoke-to-hub tunnel with mode-cfg enabled for IP address assignment, while BGP on loopback uses a single iBGP session per hub terminating on a loopback interface to simplify configuration and reduce advertised routes.

B. BGP per overlay establishes a single iBGP session per hub on a loopback interface, while BGP on loopback requires mode-cfg for IP address assignment and uses multiple iBGP sessions per tunnel.

C. BGP per overlay is used for loopback interfaces to reduce routes, while BGP on loopback is the

default method requiring separate iBGP sessions for each spoke.

D. BGP per overlay simplifies hub configuration without mode-cfg, while BGP on loopback establishes multiple iBGP sessions for each tunnel to increase advertised routes.

Answer: A

Explanation:

FortiSASE supports two main routing design methods for Secure Private Access (SPA) when connecting to a FortiGate SD-WAN hub:

BGP per Overlay (Traditional/Default Method): In this configuration, a separate iBGP session is established over every individual IPsec overlay (tunnel) between the FortiSASE PoP and the hub. These sessions terminate on the tunnel interface IP addresses. To facilitate this, the hubs typically use the IPsec VPN mode-cfg feature to dynamically assign tunnel IP addresses to the SASE PoPs. For every LAN prefix, the system generates multiple BGP routes—one for each overlay—which increases the total number of routes advertised across the network.

BGP on Loopback (Modern Alternative): This newer design establishes only a single iBGP session between the spoke and the hub, regardless of how many physical or logical overlays (tunnels) connect them. The session is terminated on a loopback interface on both sides.

Key Advantages of BGP on Loopback:

Reduced Complexity: It significantly simplifies the BGP configuration because there are fewer neighbors to manage.2
Improved Scalability: It greatly reduces the volume of routes advertised, as only a single BGP route is generated for each LAN prefix, making it the preferred choice for large-scale deployments.

Resiliency: The BGP session remains active as long as the loopback is reachable via any of the available overlays, meaning no BGP convergence is required if a single overlay fails.

Question: 70

One user has reported connectivity issues; no other users have reported problems. Which tool can the administrator use to identify the problem? (Choose one answer)

A. Mobile device management (MDM) service to troubleshoot the connectivity issue.

B. Digital experience monitoring (DEM) to evaluate the performance metrics of the remote computer.

C. Forensics service to obtain detailed information about the user's remote computer performance.

D. SOC-as-a-Service (SOCaaS) to get information about the user's remote computer.

Answer: B

Explanation:

In a FortiSASE deployment, Digital Experience Monitoring (DEM) is the primary diagnostic tool used to troubleshoot connectivity and performance issues specifically for a single user or endpoint.

End-to-End Visibility: DEM provides real-time, end-to-end visibility into the network path between the end-user's device and the application they are trying to reach. This is critical when only one user reports an issue, as it allows administrators to pinpoint whether the problem resides on the local device, the local ISP, the SASE backbone, or the destination application.

Performance Metrics: The DEM agent (often integrated with the FortiMonitor agent on the endpoint) collects granular performance metrics such as latency, jitter, packet loss, and RTT (Round Trip Time). It also provides device-specific health data, including CPU and memory usage, to determine if the connectivity issue is actually caused by the remote computer's performance.

Hop-by-Hop Analysis: Unlike standard monitoring, DEM offers End-to-End Continuous Hop Analytics. This path monitoring visualizes every "hop" in the traffic route and highlights exactly where degraded service is occurring. For a single user experiencing issues while everyone else is fine, this tool immediately triangulates if a specific "problem hop" in their unique connection path is the cause.

Operational Comparison: * MDM (A) is used for managing device configurations and software distribution, not for real-time network performance troubleshooting.

Forensics (C) is a security-focused service used for investigating malware incidents or data breaches, not for measuring network latency.

SOCaaS (D) is a managed security service for threat monitoring and event triage; while it handles "security" connectivity issues (like a blocked IP), it is not a tool for performance metric evaluation.

Question: 71

What is the maximum number of Secure Private Access (SPA) service connections (SPA hubs) supported in the SPA use case? (Choose one answer)

A. 8

B. 12

C. 4

D. 16

Answer: B

Explanation:

In recent versions of FortiSASE (starting from version 24.4 and later), the platform has increased its scalability to support larger enterprise environments.

Maximum Hub Support: According to the FortiSASE Mature Administration Guide and the FortiSASE 25.3.148 Feature Release Notes, administrators can now configure a maximum of 12 SPA Service Connections (SPA hubs). Previously, this limit was restricted to 4 hubs.

Scalability for Large Enterprises: This enhancement allows organizations with complex, geographically dispersed networks—such as those with multiple regional datacenters or cloud hubs—to integrate up to 12 distinct FortiGate SD-WAN hubs into their SASE infrastructure.

Service Connection Licensing: Each SPA hub requires a dedicated FortiGate SPA Service Connection license. In MSSP environments using FortiCloud Organizations, a single FortiSASE instance can inherit these licenses from a root OU, supporting up to the same cumulative maximum of 12 service connections.

Routing and Performance: These 12 hubs form the "Private Access" backbone, where FortiSASE security PoPs act as spokes. The use of BGP (either per-overlay or on loopback) ensures that traffic is dynamically routed to the optimal hub based on the destination network and defined SLA priorities.

Question: 72

An existing Fortinet SD-WAN customer is reviewing the FortiSASE ordering guide to identify which add-on is needed to allow future FortiSASE remote users to reach private resources. Which add-on should the customer consider to allow private access? (Choose one answer)

A. FortiSASE Global add-on

B. FortiSASE Branch On-Ramp add-on

C. FortiSASE SPA add-on

D. FortiSASE Dedicated Public IP Address add-on

Answer: C

Explanation:

To enable remote users to access internal applications located behind an existing FortiGate SD-WAN hub, the customer must license the FortiSASE Secure Private Access (SPA) add-on.

Secure Private Access (SPA) Use Case: This specific add-on is designed to extend the Fortinet Security Fabric into the SASE cloud, allowing for a hub-and-spoke architecture where the FortiSASE PoPs act as spokes and the customer's on-premises FortiGate acts as the hub.

Licensing Requirements: The SPA add-on is a per-hub (per service connection) license. It provides the necessary entitlements to establish IPsec tunnels and BGP peering between the SASE infrastructure and the corporate FortiGate.

Feature Enablement: Once the SPA license is applied, the Configuration > Private Access menu becomes available in the FortiSASE portal. This allows administrators to define "Service Connections" to their private data centers or cloud VPCs.

Analysis of Other Options:

Option A: The Global add-on is typically related to expanding the geographic reach or performance of the SASE PoPs, not specifically for private resource routing.

Option B: The Branch On-Ramp refers to connecting physical office locations (Thin Edge) to SASE, rather than the specific licensing for private application access for remote users.

Option D: Dedicated Public IP Address is used for source IP anchoring (SIA) to ensure remote users egress with a consistent IP for third-party SaaS IP-whitelisting.

Question: 73

What action must a FortiSASE customer take to restrict organization SaaS access to only FortiSASE- connected users? (Choose one answer)

A. Implement a CNAPP solution to allowlist the users under the FortiSASE egress IP

B. Implement ZTNA for their private apps and allow list them under SaaS portals or grant them conditional access.

C. Connect FortiSASE to an SPA hub for private access to an allowlisted connecting IP.

D. Retrieve the PoPs of the users' public IP addresses from the FortiSASE region IP list and whitelist the IP under SaaS

portals, or grant them conditional access.

Answer: D

Explanation:

To ensure that organizational SaaS applications (such as Microsoft 365, Salesforce, or AWS Console) are only accessible to users who are currently connected and protected by FortiSASE, administrators utilize Source IP Anchoring and IP-based access control.

Consistent Egress IPs: Every FortiSASE instance is assigned a set of dedicated public IP addresses (egress IPs) for each Security Point of Presence (PoP). Regardless of where a remote user is physically located, when they connect to a specific FortiSASE PoP, all their traffic destined for the internet or SaaS applications will appear to originate from that PoP's dedicated egress IP.

Whitelisting and Conditional Access: Administrators can retrieve the list of these dedicated egress IPs from the FortiSASE portal (typically found under the Support or Region IP list). These IPs are then configured as "Trusted Locations" or "Named Locations" within the SaaS provider's security settings (e.g., Microsoft Entra ID Conditional Access).

Enforcement Mechanism: Once the SaaS portal is configured to only permit logins from the FortiSASE egress IP ranges, any user attempting to access the application without being connected to the FortiSASE VPN will be denied access because their source IP will be their local ISP address rather than the trusted SASE IP. This effectively mandates the use of the SASE security stack for all corporate SaaS

interactions.

Analysis of Incorrect Options:

Option A: CNAPP (Cloud-Native Application Protection Platform) is used for securing cloud-native applications and infrastructure, not for managing egress IP whitelisting for external SaaS providers.

Option B: While ZTNA is a secure access method, it is primarily used for Private Applications hosted by the organization, not for third-party public SaaS portals which rely on standard IP or identity-based conditional access.

Option C: SPA hubs are designed for Secure Private Access (connecting to a corporate data center), not for managing access to public SaaS applications.

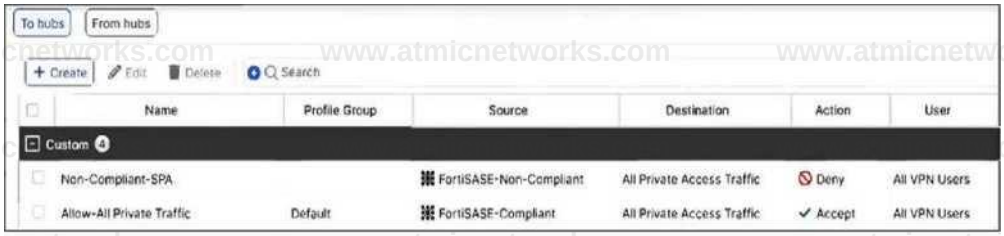
Question: 74

Refer to the exhibits.

Network diagram

JwaTMtll^ • fcrtiSWf Canplune

Private access policy on FortiSASE



BGP route information on FortiSASE

LEARNED BGP ROUTES ITO.HUBjVAhCOUVER ■ CANADA)

(OO|.arch

Prefa *	V	Nexi Hop •	Leame.a from 4
10.160.1600/24		10.11.111	10.11.11.1
100 65.170/24		0.0.00	0.000
100 65.32 0/20		0.000	000.0
100,65.176-0/20		00.0,0	o.c.o.o
100.65.17.0/24		00.0 0	0.00.0
100.65.32.0/20		00.00	o.c.o.o
100,65.176.0/20		0.0.00	0.00,0

Hub firewall policy

```
4 show firewall policy config firewall
policy
    edit 7
        set name ''vpn_Hub_spoke2bub_0" set
        srcintf "Hub" set dstintf
        "internal!" set action accept
        set srcaddr "5ASE_Resote_Acce$s" set
        dstaddr "LAN"
        set schedule "always" set service
        "ALL"
     next
end

# show firewall address
config firewall address edit "LAN"
       set subnet 10.168.168.6 255.255.255.0
    next
    edit "SASE Remote Access"
      set subnet 10.11.11.0 255.255.255.0
    next
```

Advertised routes on Hub

4 get router info bgp neighbors 10.11 11,10 advertised-"OUtes
VRF fl BGP table version is 4, local router ID Is 16.1.0.254

Status codes: s suppressed, d damped h history* • valid, > best 1 internal
Origin codes: 1 TGP, e EOF, 2 incomplete

Network	Next Hop	Metric	LocPrf	Weight	RouteTag Path
•>i lfl.12.11.1/32	10.11.11.13		100	0	0 i <■/!>
->i 10.12.11.2/32	10-11.11.12		100	fl	0 i <-/!>
->i 10.12,11.4/12	10.11,11.11		100	0	0 i <-/!>
•Xi 10.160.160.0/24 10.11,11.1			100	32768	e i </!>
■>i 100.65.17.fl/24	10,11.11.11		100	0	0 i <■/!>
•xi 100.65.18.0/24 10.11.11.13			100	B	0 i <•/!>
•xi 100.65,20.0/24 10.11.11.12			100	0	0 i o/lx
•>i 100,65.32.0/20 10.11.11.11			160	0	0 i <■/!>
•xi 100 65,48,0/20 10.11.11.12			100	0	0 i < /!>
">i 100.65.128.0/20 10-11.11.12			180	0	a i </!>
■>i 103.65,144.0/20 10.11.11.13			100	fl	0 1 <-/!>
'>1 100.65.160.0/20 10,11.11.13			100	0	0 I <■/!>
■>i 180.65.176.0/20 10.11.11.11			100	0	9 i <fix

A FortiSASE administrator has configured FortiSASE as a spoke to a FortiGate hub. The tunnel is up to the FortiGate hub. However, the remote FortiClient is not able to access the web server hosted behind the FortiGate hub. What is the reason for the access failure? (Choose one answer)

A. The hub is not advertising the required routes.

B. A private access policy has denied the traffic because of failed compliance.

C. The hub firewall policy does not include the FortiClient address range.

D. The server subnet BGP route was not received on FortiSASE.

Answer: C

Explanation:

Based on the detailed analysis of the provided exhibits (image_65feb6.jpg), the connectivity failure is caused by a mismatch in the Hub firewall policy configuration.

Endpoint Analysis: The Network Diagram shows the FortiClient endpoint has an IP address of 100.65.80.2/20 and currently carries the FortiSASE-Compliant ZTNA tag.

FortiSASE Policy Validation: The Private access policy on FortiSASE shows an "Accept" rule for traffic originating from "FortiSASE-Compliant" sources destined for "All Private Access Traffic". This confirms the traffic is successfully leaving the FortiSASE PoP.

Routing Validation: The Learned BGP Routes on FortiSASE table shows the prefix 10.160.160.0/24 (the Server subnet) is correctly received via Next Hop 10.11.11.1. Routing is correctly established.

Hub Firewall Policy Error: Examining the Hub firewall policy (edit 7), the srcaddr is set to "SASE_Remote_Access". Looking at the address object definition for "SASE_Remote_Access," it is configured with the subnet 10.11.11.0 255.255.255.0.

The Conflict: The FortiClient's actual IP address (100.65.80.2) does not fall within the 10.11.11.0/24 range defined in the policy's source address. On a FortiGate hub, for traffic to be permitted through the tunnel to the internal server, the firewall policy must include the specific subnet assigned to the remote clients, not just the tunnel interface subnet. Because the FortiClient address range is missing from the hub's policy, the traffic is dropped at the hub.

Question: 75

What is the purpose of security posture tagging in ZTNA? (Choose one answer)

A. To assign usernames to different devices for security logs

B. To ensure that all devices and users are monitored continuously

C. To provide granular access control based on the compliance status of devices and users1

D. To categorize devices and users based on their role in the organization

Answer: C

Explanation:

In the context of Zero Trust Network Access (ZTNA), security posture tagging is the fundamental mechanism used to enforce compliance and security standards before granting access to protected resources.

Granular Access Control: The primary purpose of tagging is to provide granular access control.3 Instead of relying solely on static credentials, ZTNA uses these dynamic tags to determine if a device or user meets specific security requirements at the moment of the connection request.

Compliance-Based Enforcement: Tags are assigned based on the compliance status of the endpoint. For example, the FortiSASE Endpoint Management Service (EMS) can verify if a device has an active antivirus, is running a specific OS version, or is joined to the corporate domain.5 If the device fails any of these checks, the "Compliant" tag is removed, and access is automatically revoked.

Dynamic and Continuous Assessment: Unlike traditional VPNs that check posture only at login, ZTNA posture tagging allows for continuous assessment. If a device's security posture changes—for instance, if the user disables their firewall—the tag is updated in real-time across the Security Fabric, and the ZTNA policy will immediately deny further access.8

Integration with Policies: On the FortiGate (acting as a ZTNA proxy) or within FortiSASE, these tags are used as source criteria in ZTNA policies.9 Only traffic originating from endpoints with the required tags (e.g., "EMS-Tag: Corporate-Managed") is permitted to reach the protected application.

Question: 76

Refer to the exhibits.

Endpoint Profile

Sean for Vulnerabilities

Scheduled scanning	C	
Schedule type	Weekly	*
Scan on	Sunday	•
Start at	12-00 AM	O
Event-based scanning ©	O	
Automatically patch vulnerabilities ©	O	

Vulnerability Dashboard

AP9UCATI0NS VUMWBUITIES

VuTttKxMyS	Category 8	Seventy •	CWt	^chng itititrt
FoivCMM CvE 2024 $0564 Information Disclosure vunereOMy	AppScetiont		CW-2024 50564	Mvrua peter v«g >eqwed
OpenSSL CW-2023 «2a0em»i el Service VWweMty	ApptUUttH		CW-2023 5676	Mir uji patcr*^ reowj rd
□ Setirty Vumeut»Hi»i Inert m VMwere tWrkSUtion Player WSA 2025 0004	AppScetions		CW 2025 22226 CVE 20-	MenuM pattNng lequved

How will the application vulnerabilities be patched, based on the exhibits provided? (Choose one answer)

A. An administrator will patch the vulnerability remotely using FortiSASE.

B. The end user will patch the vulnerabilities using the FortiClient software.

C. The vulnerability will be patched by installing the patch from the vendor's website.

D. The vulnerability will be patched automatically based on the endpoint profile configuration.

Answer: A

Explanation:

Based on the settings shown in the provided exhibits, the vulnerability remediation workflow is determined by the Endpoint Profile and the Vulnerability Dashboard.

Endpoint Profile Evaluation: The top exhibit displays the Scan for Vulnerabilities settings. The toggle for Automatically patch vulnerabilities is explicitly set to Disabled. Consequently, the system will not perform automated remediation when a scan completes.

Manual Patching Requirement: The Vulnerability Dashboard (bottom exhibit) lists several application vulnerabilities with a Patching status of Manual patching required. In a FortiSASE environment, "Manual" indicates that the vulnerability cannot be handled by the client's autonomous update process and requires a direct instruction from the management plane.

Administrative Intervention: The dashboard includes a Patch endpoints action button. Since autopatching is disabled in the profile, an administrator must manually select the vulnerabilities and click the "Patch endpoints" button to remotely trigger the patching sequence on the managed endpoints via the FortiSASE cloud service.

Workflow Logic: While FortiClient acts as the "conductor" on the local machine to facilitate the download and installation, the trigger for this specific scenario is the administrator's remote action within the portal. This differentiates it from Option D (which is disabled) and Option C (which would involve a user manually browsing a website outside the managed SASE workflow).

Question: 77

Which information does FortiSASE use to bring network lockdown into effect on an endpoint? (Choose one answer)

A. Zero-day malware detection on endpoint

B. The number of critical vulnerabilities detected on the endpoint

C. The connection status of the tunnel to FortiSASE

D. The security posture of the endpoint based on ZTNA tags

Answer: C

Explanation:

The Network Lockdown feature in FortiSASE is a specialized security control designed to ensure that managed endpoints remain protected by the SASE security stack at all times.

Mechanism of Action: Network lockdown relies specifically on the connection status of the tunnel to FortiSASE. When this feature is enabled in the Endpoint Profile, the FortiClient agent monitors whether the secure VPN tunnel (SSL or IPsec) to a FortiSASE Point of Presence (PoP) is active.

Enforcement Logic: If the agent detects that the tunnel is disconnected, it immediately places the endpoint's network

interface into a "locked" state. In this state, all inbound and outbound network traffic is blocked, with the exception of traffic required to re-establish the connection to the FortiSASE infrastructure.

Purpose: This prevents "leakage" where an endpoint might communicate directly with the internet without inspection if the VPN tunnel drops or is manually disabled by the user. It essentially mandates that the device is either connected to FortiSASE or has no network access at all.

Analysis of Incorrect Options:

Option A and B: While malware and vulnerabilities affect the security posture, they trigger different remediation actions (like quarantine or patching) rather than the "Network Lockdown" tunnel-state feature.

Option D: ZTNA tags identify the security posture to allow or deny access to specific applications, whereas Network Lockdown is a binary state (On/Off) affecting all network traffic based purely on tunnel connectivity.

Question: 78

A company must provide access to a web server through FortiSASE secure private access for contractors. What is the recommended method to provide access? (Choose one answer)

A. Configure a TCP access proxy forwarding rule and push it to the contractor FortiClient endpoint.

B. Publish the web server URL on a bookmark portal and share it with contractors.

C. Update the PAC file with the web server URL and share it with contractors.

D. Update the DNS records on the endpoint to access private applications.

Answer: B

Explanation:

When providing Secure Private Access (SPA) to external contractors who may not be using managed corporate devices, FortiSASE offers specific methods to ensure security while maintaining ease of use.

Bookmark Portal (Clientless Access): For web-based resources like a web server, the recommended and most efficient method for contractors is to use the ZTNA portal (bookmark portal). This allows for clientless access, meaning the contractor does not need to install the FortiClient agent or any specific software on their personal machine.

Workflow: The administrator publishes the web server URL as a bookmark within the FortiSASE portal. Contractors simply log into the secure SASE web portal via their browser, authenticate, and click the bookmark to access the internal

server.

Security Benefits: This method leverages the FortiSASE ZTNA access proxy to mediate the connection. It ensures that the contractor is authenticated and that the traffic is inspected without exposing the internal network directly to the contractor's device.

Analysis of Incorrect Options:

Option A: TCP forwarding rules require the FortiClient agent to be installed and managed on the endpoint. Contractors often use unmanaged devices where installing agents is restricted or undesirable.

Option C: Updating a PAC (Proxy Auto-Configuration) file is part of a Secure Web Gateway (SWG) deployment for internet access, not for routing traffic to private internal web servers via an SPA hub.1

Option D: Manually updating DNS records on a contractor's endpoint is an unscalable, insecure, and administratively heavy task that does not provide the session-level security required by ZTNA.

Question: 79

What happens to the logs on FortiSASE that are older than the configured log retention period? (Choose one answer)

A. The logs are deleted from FortiSASE.1

B. The logs are compressed and archived.

C. The logs are backed up on FortiCloud.

D. The logs are indexed and can be stored in a SQL database.

Answer: A

Explanation:

In a FortiSASE environment, log management is governed by a cloud-native storage policy that prioritizes performance and resource availability.

Retention Policy Framework: All FortiSASE instances come with log retention enabled by default. The standard log retention period is 30 days, though administrators can customize this policy to any duration between 2 and 30 days. This policy applies across all log types, including traffic, security, and event logs.

Automatic Deletion (A): When logs exceed the configured retention threshold, FortiSASE automatically deletes the older logs from the platform.2 This automatic purging is necessary to free up storage space on the cloud infrastructure and maintain compliance with the organization's data lifecycle settings.

Persistence and Recovery: Once logs are deleted due to the expiration of the retention period, they are generally unrecoverable from the FortiSASE platform.

Long-Term Storage Solutions: Because FortiSASE is not designed as a long-term archival solution, customers who need to store logs for months or years for regulatory compliance should configure log forwarding to an external server, such as a FortiAnalyzer or a remote Syslog server.

Analysis of Incorrect Options: * Option B and D: While traditional FortiAnalyzer deployments use SQL indexing and separate "Archive" (raw/compressed) vs. "Analytics" (SQL) tiers, FortiSASE uses a simplified cloud storage model where data is purged rather than archived or tier-shifted upon expiry.

Option C: While FortiSASE is part of the FortiCloud ecosystem, it does not automatically "back up" expired logs to another FortiCloud service; the deletion is final unless external forwarding is active.

Question: 80

A FortiSASE administrator is receiving reports that some users have travelled overseas and cannot establish their agent-based VPN tunnels, although they can authenticate with their SSO credentials to access O365 and SFDC directly. The administrator reviewed the firewall policies and ZTNA tags of some users and could not find anything unusual. Which action can the administrator take to resolve

this problem? (Choose one answer)

A. Create a dedicated firewall policy for the users.

B. Instruct the users to restart their laptops and log in again.

C. Ensure that the countries the users are visiting are not listed under the Deny list in the Geofencing settings.

D. Instruct the users to install the updated version of the agent-based client.

Answer: C

Explanation:

In a FortiSASE environment, the ability of a remote user to establish a VPN tunnel is governed not only by their credentials and firewall policies but also by geographic access controls.

Geofencing Mechanism: FortiSASE includes a Geofencing feature (found under Configuration > Restrictions or Configuration > Geofencing in newer versions) that allows administrators to restrict or allow access to SASE services based on the geographic location of the endpoint's public IP address.

Connection Failure vs. SSO Success: The scenario describes a situation where users can successfully authenticate via SSO to reach third-party SaaS apps like Office 365 (O365) or Salesforce (SFDC) but cannot connect to the SASE VPN. This occurs because the SSO authentication is handled directly by the Identity Provider (IdP) (e.g., Microsoft Entra ID), which may not have the same geographic restrictions. However, when the FortiClient attempts to establish the tunnel to the FortiSASE Point of Presence (PoP), the SASE gateway checks the Geofencing list. If the country the user is visiting is on the Deny list (or not on the Allow list), the connection is dropped at the "local-in" policy level on the SASE backend, preventing the tunnel from forming.

Verification and Resolution: To resolve this, the administrator must verify the Geofencing settings and ensure that the countries where the traveling users are located are permitted to connect. If the feature is enabled with a "Deny" list, the specific country must be removed from that list; if it uses an "Allow" list, the country must be added.

Analysis of Other Options:

Option A: Firewall policies govern traffic after the tunnel is established; they cannot resolve a failure to connect the tunnel itself.

Option B: Restarting the device is a general troubleshooting step but will not bypass a server-side geographic block.

Option D: While keeping clients updated is a best practice, the issue described (specific to overseas travel while other functions work) points to a configuration restriction rather than a software bug.

Question: 81

In the Secure Private Access (SPA) use case, which two FortiSASE features facilitate access to corporate applications? (Choose two answers)

A. SD-WAN

B. zero trust network access (ZTNA)

C. thin edge

D. cloud access security broker (CASB)

Answer: A, B

Explanation:

In a FortiSASE deployment, the Secure Private Access (SPA) use case is specifically designed to provide remote users with secure, high-performance connectivity to internal corporate applications hosted in private data centers or public clouds.5 This is achieved through two primary architectural methods:

SD-WAN Integration (A): FortiSASE integrates natively with existing Fortinet Secure SD-WAN networks.6 In this architecture, the FortiSASE global PoPs act as spokes that establish automated IPsec tunnels to the organization's FortiGate SD-WAN hubs. This allows the platform to use intelligent application steering and dynamic routing to find the shortest, most efficient path to private resources, ensuring a superior user experience.

Zero Trust Network Access (ZTNA) (B): FortiSASE provides Universal ZTNA to enforce granular, persession access control.7 Unlike traditional VPNs that grant broad network access, ZTNA verifies the user's identity and the endpoint's security posture (via ZTNA tags) before every application session. This ensures that users only have access to the specific corporate applications they are authorized to

use, significantly reducing the attack surface.

Analysis of Other Options: * Thin Edge (C) is a connectivity method used to secure branch offices and micro-branches (typically using FortiExtender), rather than a specific feature for facilitating private corporate application access for individual remote users.

CASB (D) is used for Secure SaaS Access (SSA) to provide visibility and control over third-party cloud applications like Office 365, rather than private applications hosted on-premises.