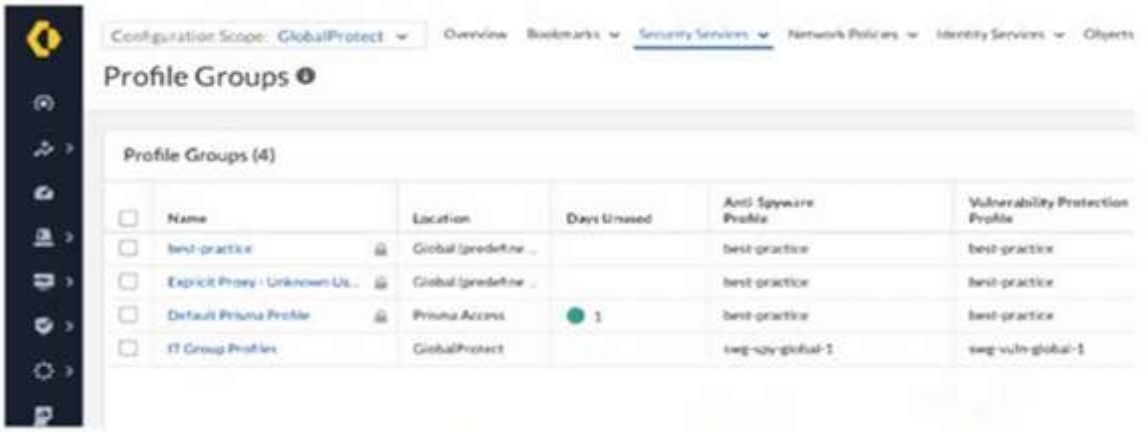
QUESTION 1
A large retailer has deployed all of its stores with the same IP address subnet. An engineer is onboarding these stores as Remote Networks in Prisma Access. While onboarding each store, the engineer selects the "Overlapping Subnets" checkbox. Which Remote Network flow is supported after onboarding in this scenario?

A. To private applications
B. To the internet
C. To remote network
D. To mobile users

Answer: A
Explanation:
When the "Overlapping Subnets" checkbox is selected during the Remote Network onboarding process in Prisma Access, the deployment enables Private Application access using Prisma Access for Users (ZTNA or Private Access). This feature is designed to handle scenarios where multiple sites use the same IP subnet by leveraging NAT (Network Address Translation) and segmentation to avoid conflicts.
Since overlapping subnets can create routing challenges for direct remote network-to-remote network communication, Prisma Access does not support Remote Network-to-Remote Network or Mobile User communication in this case.
Private application access is supported as Prisma Access correctly routes requests based on application-layer intelligence rather than IP-based routing.

QUESTION 2
An intern is tasked with changing the Anti-Spyware Profile used for security rules defined in the GlobalProtect folder. All security rules are using the Default Prisma Profile. The intern reports that the options are greyed out and cannot be modified when selecting the Default Prisma Profile.
Based on the image below, which action will allow the intern to make the required modifications?



A. Request edit access for the GlobalProtect scope.
B. Change the configuration scope to Prisma Access and modify the profile group.
C. Create a new profile, because default profile groups cannot be modified.
D. Modify the existing anti-spyware profile, because best-practice profiles cannot be removed from a group.

Answer: C
Explanation:
Palo Alto Networks best practices and the behavior of Strata Cloud Manager (SCM) dictate that predefined or default objects, including profile groups like "Default Prisma Profile," cannot be directly modified. These default objects serve as baseline configurations and are often locked to prevent accidental or unintended changes that could impact the overall security posture. The intern's experience of the options being greyed out when selecting "Default Prisma Profile" is a direct indication of this immutability of default objects.
Configure the new Profile Group: In this new profile group, the intern can select the desired Anti- Spyware Profile (which might be an existing custom profile or a new one they create). Modify Security Rules: The security rules currently using the "Default Prisma Profile" in the GlobalProtect folder need to be modified to use this newly created profile group.

QUESTION 3
How can role-based access control (RBAC) for Prisma Access (Managed by Strata Cloud Manager) be used to grant each member of a security team full administrative access to manage the Security policy in a single tenant while restricting access to other tenants in a multitenant deployment?

A. Add the team to the Parent Tenant, select the Prisma Access Configuration Scope, and set the role to Security Administrator.
B. Add the team to the Child Tenant, select All Apps & Services, and set the role to Security Administrator.
C. Add the team to the Parent Tenant, select Prisma Access & NGFW Configuration, and set the role to Security Administrator.
D. Add the team to the Child Tenant, select Prisma Access & NGFW Configuration, and set the role to Security Administrator.

Answer: D
Explanation:
In a multitenant deployment, access control must be configured at the Child Tenant level to ensure that security administrators have full control over Security policy only within their assigned tenant while restricting access to other tenants. By selecting Prisma Access & NGFW Configuration, the assigned users gain full administrative access only for security policy management within the designated tenant, aligning with RBAC best practices for controlled access in Prisma Access Managed by Strata Cloud Manager.

QUESTION 4
An engineer configures a Security policy for traffic originating at branch locations in the Remote Networks configuration scope. After committing the configuration and reviewing the logs, the branch traffic is not matching the Security policy. Which statement explains the branch traffic behavior?

A. The source address was configured with an address object including the branch location prefixes.
B. The source zone was configured as "Trust."
C. The Security policy did not meet best practice standards and was automatically removed.
D. The traffic is matching a Security policy in the Prisma Access configuration scope.

Answer: D
Explanation:
In Prisma Access, security policies are evaluated based on their configuration scope. If the engineer configured a Security policy under the Remote Networks scope, but traffic from the branch locations is instead matching a Security policy under the Prisma Access configuration scope, the intended policy will not take effect. This happens because Prisma Access evaluates security rules based on the highest-level applicable configuration first, which can override more specific Remote Networks policies.

QUESTION 5
What is the flow impact of updating the Cloud Services plugin on existing traffic flows in Prisma Access?

A. They will experience latency during the plugin upgrade process.
B. They will automatically terminate when the upgrade begins.
C. They will be unaffected because the plugin upgrade is transparent to users.
D. They will be unaffected only if Panorama is deployed in high availability (HA) mode.

Answer: C
Explanation:
Updating the Cloud Services plugin in Prisma Access does not disrupt existing traffic flows because the upgrade process is designed to be seamless and transparent. Prisma Access ensures high availability by maintaining active sessions and policies while applying the update in the background. This allows ongoing connections to continue without interruptions, minimizing impact on user experience.

QUESTION 6
Which overlay protocol must a customer premises equipment (CPE) device support when terminating a Partner Interconnect-based Colo-Connect in Prisma Access?

A. Geneve
B. IPSec
C. GRE
D. DTLS

Answer: B
Explanation:
When terminating a Partner Interconnect-based Colo-Connect in Prisma Access, the Customer Premises Equipment (CPE) must support IPSec as the overlay protocol. Prisma Access establishes secure IPSec tunnels between the Colo-Connect infrastructure and the CPE, ensuring encrypted communication and reliable connectivity. IPSec provides secure site-to-cloud integration, enabling customers to extend their private network securely over the Prisma Access infrastructure.

QUESTION 7
Which policy configuration in Prisma Access Browser (PAB) will protect an organization from malicious BYOD and minimize the impact on the user experience?

A. One that blocks file exchange
B. One for session recording
C. One that blocks elements such as screen scrapers
D. One that allows access to applications with data masking or watermarking

Answer: D
Explanation:
In Prisma Access Browser (PAB), allowing access to applications while enforcing data masking or watermarking provides security for BYOD (Bring Your Own Device) users without heavily impacting the user experience. Data masking ensures that sensitive information is obscured, reducing the risk of data leakage, while watermarking can deter unauthorized screenshots or data exfiltration. This approach balances security and usability, allowing users to work efficiently while protecting corporate data.

QUESTION 8
During a deployment of Prisma Access (Managed by Strata Cloud Manager) for mobile users, a SAML authentication type and authentication profile in the Cloud Identity Engine application is successfully created.
Using this SAML authentication, what is a valid next step to configure authentication for mobile users?

A. Perform a full commit to Strata Cloud Manager so the Cloud Identity Engine profiles get synchronized from the application.
B. Permit the Cloud Identity Engine service account RBAC access to the mobile user folder in Strata Cloud Manager.

C. In Strata Cloud Manager, create a new authentication type of "Cloud Identity Engine."
D. Create a SAML authentication profile in Strata Cloud Manager and link it to the Cloud Identity Engine profile.

Answer: D
Explanation:
After successfully creating a SAML authentication type and authentication profile in Cloud Identity Engine, the next step is to configure a corresponding SAML authentication profile in Strata Cloud Manager and link it to the Cloud Identity Engine profile. This ensures that Prisma Access (Managed by Strata Cloud Manager) can authenticate mobile users using the configured SAML identity provider (IdP), enabling seamless user authentication and access control.

QUESTION 9
After configuring domain-based split tunnel for zoom.us, how is expected behavior on the client machine confirmed?

A. Verify from the routing table.
B. Enable dump level logs on GlobalProtect Application.
C. Verify zoom.us is resolved by the tunnel assigned DNS server.
D. Ping zoom.us from the CLI.

Answer: A
Explanation:
After configuring domain-based split tunneling for zoom.us, the expected behavior can be confirmed by checking the routing table on the client machine. If split tunneling is correctly configured, the traffic for zoom.us should be routed outside the GlobalProtect VPN tunnel, while other traffic follows the tunnel path. Reviewing the routing table ensures that only the intended traffic is excluded from the tunnel, confirming that the split tunnel configuration is working as expected.

QUESTION 10
Which Cloud Identity Engine capability will create a Security policy that uses Entra ID attributes as the source identification?

A. Entra ID Group Attribute
B. Attribute Group Mapping
C. Entra ID Cloud Group
D. Cloud Dynamic User Group

Answer: D
Explanation:
The Cloud Dynamic User Group capability in Cloud Identity Engine enables the creation of Security policies that use Entra ID (formerly Azure AD) attributes for user identification. This allows Prisma Access to dynamically apply user-based security rules based on real-time Entra ID attributes, ensuring that access policies adapt to user changes such as group membership, device compliance, or role updates.

QUESTION 11
An engineer deploys a new branch connected to Prisma Access. From the customer premises equipment (CPE) device at the branch, Phase 1 on the tunnel is established, but Phase 2-encrypted packets are not coming back from Prisma Access.
Which Strata Logging Service log facility should the engineer review to determine why Phase 2- encrypted traffic is not being received?

A. Decrypt logs
B. System logs
C. Traffic logs
D. Tunnel logs

Answer: D
Explanation:
Since Phase 1 of the IPSec tunnel is established but Phase 2 traffic is not being received, the Tunnel logs in Strata

Logging Service should be reviewed. Tunnel logs provide visibility into IPSec tunnel establishment, Phase 2 negotiation, and any errors or dropped packets related to encrypted traffic. This will help identify whether ESP (Encapsulating Security Payload) traffic is being blocked, mismatched security associations (SAs) exist, or if there are other issues with Prisma Access responding to Phase 2-encrypted packets.

QUESTION 12
When configuring Remote Browser Isolation (RBI) with Prisma Access (Managed by Strata Cloud Manager), which element is required to define the protected URLs for mobile users?

A. A URL access management profile with site access set to "Isolate" applied to a Security policy
B. A DNS Security profile applied to a Security policy with the action of "Isolate" for the target remote browser DNS categories
C. An RBI profile applied to the URL access management profile
D. A Security policy with the target URL categories and set the action to "Isolate"

Answer: A
Explanation:
When configuring Remote Browser Isolation (RBI) in Prisma Access (Managed by Strata Cloud Manager) for mobile users, a URL access management profile must be created with the site access action set to "Isolate". This profile is then applied to a Security policy to enforce isolation for specific URLs. This ensures that web traffic to designated high-risk or untrusted sites is redirected to a remote, secure browser instance, protecting endpoints from potential web-based threats.

QUESTION 13
A malicious user is attempting to connect to a blocked website by crafting a packet using a fake SNI and the correct website in the HTTP host header.
Which option will prevent this form of attack?

A. Advanced Threat Prevention option to block "Domain Fronting"
B. Advanced URL Filtering and block the "Malicious Behavior" category
C. Advanced URL Filtering and block "SNI mismatch with Server Certificate (SAN/CN)"
D. SSL Decryption to "Block sessions on SNI mismatch with Server Certificate (SAN/CN)"

Answer: D
Explanation:
This option ensures that SSL Decryption checks for mismatches between the Server Name Indication (SNI) field in the TLS handshake and the Common Name (CN) or Subject Alternative Name (SAN) in the server certificate. If a malicious user tries to bypass content filtering by spoofing the SNI while using the real blocked website in the HTTP host header, this setting will detect the discrepancy and block the session, preventing unauthorized access.

QUESTION 14
A user connected to Prisma Access reports that traffic intermittently is denied after matching a Catch-All Deny rule at the bottom and bypassing HIP-based policies. Refreshing VPN connection restores the access.
What are two reasons for this behavior? (Choose two.)

A. "Collect HIP data' needs to be enabled in the configuration.
B. User mapping is learned from sources other than gateway authentication.
C. Firewall loses user mapping due to missed HIP report checks.
D. HIP-enforced policy is scheduled for certain hours of the day.

Answer: BC
Explanation:
User mapping learned from sources other than gateway authentication can cause intermittent access issues if it conflicts with the expected user identity used in HIP-based policies. If the firewall is associating the user with an outdated or incorrect mapping, traffic may not match the intended security policies, leading to denials by the Catch-All Deny rule.
If the firewall loses user mapping due to missed HIP report checks, the user may temporarily lose access to policies that require a valid Host Information Profile (HIP) match. When the VPN connection is refreshed, the HIP check is re-

initiated, restoring access until the issue repeats.

QUESTION 15
Which feature can help address a customer concern about the length of time it takes to update their SaaS-allowed IP addresses while onboarding to Prisma Access?

A. Dynamic IP pooling
B. DNS-based load balancing
C. Traffic steering
D. Dedicated IP addresses

Answer: C
Explanation:
When onboarding to Prisma Access, using Dedicated IP addresses helps address concerns about the time required to update SaaS-allowed IP lists. With dedicated egress IPs, the customer receives fixed, predictable IP addresses that do not change dynamically. This eliminates the need to frequently update SaaS providers' allowlists, ensuring seamless access to cloud applications without interruptions due to IP address changes.

QUESTION 16
Which feature within Strata Cloud Manager (SCM) allows an operations team to view applications, threats, and user insights for branch locations for both NGFW and Prisma Access simultaneously?

A. Command Center
B. Log Viewer
C. Branch Site Monitor
D. SASE Health Dashboard

Answer: A
Explanation:
The Command Center within Strata Cloud Manager (SCM) provides a centralized view of applications, threats, and user insights across both NGFW (Next-Generation Firewall) and Prisma Access simultaneously. This feature enables the operations team to monitor branch locations, analyze security events, and detect anomalies in real time, offering a comprehensive visibility and threat intelligence interface for proactive network and security management.

QUESTION 17
In addition to creating a Security policy, how can an AI Access Security be used to prevent users from uploading financial information to ChatGPT?

A. Apply File Blocking to stop file uploads containing financial information.
B. Configure an Enterprise DLP rule to block uploads containing financial information.
C. Add the ChatGPT domains using URL Filtering to block uploads containing financial information.
D. Apply a vulnerability profile to stop attempts to exploit system flaws or gain unauthorized access to financial systems.

Answer: B
Explanation:
Palo Alto Networks AI Access Security integrates with Enterprise Data Loss Prevention (DLP) capabilities to control sensitive data within AI applications like ChatGPT. The most effective way to prevent users from uploading financial information is to:
Define an Enterprise DLP rule: This rule would be configured to identify content that matches patterns or keywords associated with financial information (e.g., credit card numbers, bank account details, tax identifiers, financial statements).
Apply the DLP rule to the AI Access Security policy: This policy would be specifically configured to inspect traffic to and from ChatGPT. When the DLP rule detects a user attempting to upload content containing financial information, it can take a defined action, such as blocking the upload.

QUESTION 18
Which statement is valid in relation to certificates used for GlobalProtect and pre-logon?

A. A public certificate authority (CA) must sign and validate all certificates used.
B. The certificate used for pre-logon must include both Subject and Subject-Alt fields.
C. Certificates must be deployed in the Machine Certificate Store.
D. The GlobalProtect agent may be used to distribute pre-logon certificates.

Answer: C
Explanation:
For GlobalProtect with pre-logon, certificates must be installed in the Machine Certificate Store to ensure that authentication occurs before user login. This allows the GlobalProtect client to establish a VPN connection before the user logs in, enabling access to corporate resources such as domain controllers and authentication services. Using machine certificates ensures secure authentication and eliminates dependency on user credentials at the pre-logon stage.

QUESTION 19
What must be configured to accurately report an application's availability when onboarding a discovered application for ZTNA Connector?

A. icmp ping
B. https ping
C. tcp ping
D. udp ping

Answer: C
Explanation:
When onboarding a discovered application for ZTNA Connector, configuring a TCP ping allows Prisma Access to accurately report the application's availability. TCP ping (also known as a TCP connection check) verifies whether the application's service port is open and responsive, ensuring that the application is reachable before allowing user connections. This method is more reliable than ICMP ping, as many cloud and SaaS applications block ICMP traffic for security reasons.

QUESTION 20
All mobile users are unable to authenticate to Prisma Access (Managed by Strata Cloud Manager) using SAML authentication through the Cloud Identity Engine. Users report that after entering their credentials on the Identity Provider (IdP) login page, they are redirected to the Prisma Access portal without successful authentication, and they receive this error message:
`Error: Prisma Access Portal Authentication Failed using CIE-SAML with message "400 Bad Request"`
Which action will identify the root cause of this error?

A. Verify the SAML metadata configuration in both Strata Cloud Manager and the IdP portal to confirm that the endpoint URLs and certificates are correctly configured.
B. Examine the Security policy rules in Prisma Access to ensure that traffic from the IdP is allowed and not blocked.
C. Verify the SAML metadata configuration in both the Cloud Identity Engine and the IdP portal to confirm that the endpoint URLs and certificates are correctly configured.
D. Review the Authentication logs in Strata Cloud Manager to check for any SAML error messages or authentication failures.

Answer: C
Explanation:
The "400 Bad Request" error when attempting SAML authentication through the Cloud Identity Engine (CIE) suggests a misconfiguration in the SAML metadata.
This typically occurs when the endpoint URLs, certificates, or entity IDs do not match between Cloud Identity Engine and the IdP portal. To resolve this, verify that:
The SAML metadata uploaded to Cloud Identity Engine matches the configuration from the IdP.
The ACS (Assertion Consumer Service) URL, Entity ID, and certificate are correctly set.
There are no incorrect or expired certificates in the Cloud Identity Engine and IdP configuration.

By ensuring the SAML metadata is properly configured in both systems, authentication should proceed without errors.

QUESTION 21
An engineer has configured a new Remote Networks connection using BGP for route advertisements. The IPSec tunnel has been established, but the BGP peer is not up. Which two elements must the engineer validate to solve the issue? (Choose two.)

A. Secret
B. MRAI Timers
C. Peer AS Number
D. Advertise Default Route Checkbox

Answer: AC
Explanation:
The BGP peer not coming up despite an established IPSec tunnel indicates a potential BGP configuration issue.
Secret - If MD5 authentication is configured for BGP, both Prisma Access and the Customer Premises Equipment (CPE) must have the same secret (authentication key). A mismatch will prevent BGP from establishing a session.
Peer AS Number - The Autonomous System (AS) number of the BGP peer must match what is expected on both sides of the connection. If the AS number is incorrect, the BGP session will fail to establish.
By verifying these elements, the engineer can troubleshoot and establish a successful BGP peering session over the IPSec tunnel.

QUESTION 22
In an Explicit Proxy deployment where no agent can be used on the endpoint, which authentication method is supported with mobile users?

A. LDAP
B. Kerberos
C. SAML
D. SSO

Answer: C
Explanation:
In an Explicit Proxy deployment where no agent can be used on the endpoint, SAML (Security Assertion Markup Language) is the supported authentication method for mobile users. SAML allows authentication via an Identity Provider (IdP) without requiring an agent on the endpoint, making it ideal for web-based authentication in cloud and remote access environments. It enables Single Sign-On (SSO) and secure authentication without direct integration with LDAP or Kerberos, which typically require an agent or local network presence.

QUESTION 23
Which advanced AI-powered functionality does Strata Copilot provide to enhance the capabilities of Prisma Access security teams?

A. Real-time traffic analysis for automated threat prevention
B. Initial configuration of Prisma Access using a natural language interface
C. Customized guidance for resolving issues through recommended next steps
D. Automated remediation of misconfigured security policies

Answer: C
Explanation:
Strata Copilot enhances the capabilities of Prisma Access security teams by providing AI-powered insights and recommendations to help resolve security issues efficiently. It analyzes security events, misconfigurations, and alerts and offers contextual guidance with recommended next steps for troubleshooting and improving security posture. This assists teams in quickly identifying and addressing security challenges without requiring deep manual investigation.

QUESTION 24
Where are tags applied to control access to Generative AI when implementing AI Access Security?

A. To Generative AI applications for identifying sanctioned, tolerated, or unsanctioned applications
B. To security rules for defining which types of Generative AI applications are allowed or blocked
C. To user devices for identifying and controlling which Generative AI applications they can access
D. To Generative AI URL categories for classifying trusted and untrusted Generative AI websites

Answer: A
Explanation:
When implementing AI Access Security, tags are applied to Generative AI applications to classify them as sanctioned, tolerated, or unsanctioned. This allows organizations to enforce policy-based access control over AI tools, ensuring that only approved applications are accessible while restricting or monitoring usage of untrusted or high-risk AI platforms. This classification helps security teams manage AI-related risks and compliance effectively.

QUESTION 25
How can an engineer use risk score customization in SaaS Security Inline to limit the use of unsanctioned SaaS applications by employees within a Security policy?

A. Lower the risk score of sanctioned applications and increase the risk score for unsanctioned applications.
B. Increase the risk score for all SaaS applications to automatically block unwanted applications.
C. Build an application filter using unsanctioned SaaS as the category.
D. Build an application filter using unsanctioned SaaS as the characteristic.

Answer: A
Explanation:
SaaS Security Inline allows engineers to customize the risk scores assigned to different SaaS applications based on various factors. By manipulating these risk scores, you can influence how these applications are treated within Security policies.
To limit the use of unsanctioned SaaS applications:
Lower the risk score of sanctioned applications: This makes them less likely to trigger policies designed to restrict high-risk activities.
Increase the risk score of unsanctioned applications: This elevates their perceived risk, making them more likely to be caught by Security policies configured to block or limit access based on risk score thresholds.
Then, you would create Security policies that take action (e.g., block access, restrict features) based on these adjusted risk scores.
For example, a policy could be configured to block access to any SaaS application with a risk score above a certain threshold, which would primarily target the unsanctioned applications with their inflated scores.

QUESTION 26
Which two Prisma Access tools help troubleshoot connectivity issues for mobile users? (Select two)

A. Real-Time Monitoring and Alerting
B. Prisma Access Activity Insights
C. Secure Web Gateway
D. SaaS Security

Answer: AB

QUESTION 27
An administrator notices that Prisma Access users experience intermittent connection drops. What should be the first step in troubleshooting?

A. Reconfigure mobile user VPN settings
B. Restart all security nodes
C. Disable security policies temporarily
D. Check the Prisma Access real-time monitoring tools

Answer: D