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

A customer is implementing Prisma Access (Managed by Strata Cloud Manager) to connect mobile users, branch locations, and business-to- business (B2B) partners to their data centers.
The solution must meet these requirements:
The mobile users must have internet filtering, data center connectivity, and remote site connectivity to the branch locations.
The branch locations must have internet filtering and data center connectivity.
The B2B partner connections must only have access to specific data center internally developed applications running on non-standard ports.
The security team must have access to manage the mobile user and access to branch locations.
The network team must have access to manage only the partner access.
How should Prisma Access be implemented to meet the customer requirements?

A. Deploy two Prisma Access instances - the first with mobile users, remote networks, and private access for all internal connection types, and the second with remote networks and private application access for B2B connections - and use the Strata Multitenant Cloud Manager Prisma Access configuration scope to manage access.
B. Deploy a Prisma Access instance with mobile users, remote networks, and private access for all connection types, and use the Prisma Access Configuration scope to manage all access.
C. Deploy two Prisma Access instances - the first with mobile users, remote networks, and private access for all internal connection types, and the second with remote networks and private application access for B2B connections - and use the specific configuration scope for the connection type to manage access.
D. Deploy a Prisma Access instance with mobile users, remote networks, and private access for all connection types, and use the specific configuration scope for the connection type to manage access.

Answer: C

Explanation:
To meet the customer's requirements, two separate Prisma Access instances should be deployed:
Instance 1 should include mobile users, remote networks, and private access for internal connectivity. This ensures that mobile users can access the internet, data centers, and remote branch locations while enforcing security policies.
Instance 2 should be configured with remote networks and private application access for B2B connections. This instance will restrict access to only the required internally developed applications using non-standard ports, ensuring that partners cannot access other corporate resources.
By using specific configuration scopes for different connection types, the security team can manage access to mobile users and branch locations, while the network team can manage B2B partner connections. This ensures proper segmentation of management responsibilities while maintaining security and compliance.

Question: 2

A customer is implementing Prisma Access (Managed by Strata Cloud Manager) to connect mobile users, branch locations, and business-to- business (B2B) partners to their data centers.
The solution must meet these requirements:
The mobile users must have internet filtering, data center connectivity, and remote site connectivity to the

branch locations.
The branch locations must have internet filtering and data center connectivity.
The B2B partner connections must only have access to specific data center internally developed applications running on non-standard ports.
The security team must have access to manage the mobile user and access to branch locations.
The network team must have access to manage only the partner access.
How can the engineer configure mobile users and branch locations to meet the requirements?

A. Use GlobalProtect and Remote Networks to filter internet traffic and provide access to data center resources using service connections.
B. Use Explicit Proxy to filter internet traffic and provide access to data center resources using service connections.
C. Use GlobalProtect to filter internet traffic and provide access to data center resources using service connections.
D. Use Explicit Proxy and Remote Networks to filter internet traffic and provide access to data center resources using service connections.

Answer: A

Explanation:
To meet the customer's requirements, GlobalProtect and Remote Networks should be used as follows:
GlobalProtect: This enables secure access for mobile users, ensuring internet filtering, data center connectivity, and access to branch locations.
Remote Networks: This is used to provide security and connectivity for branch locations, ensuring internet filtering and data center access.
Service Connections: These allow both mobile users and branch locations to securely connect to the data center for internal resources.
This configuration ensures that mobile users and branch locations can securely access the internet while maintaining a segregated and secure connection to internal resources. It also aligns with Prisma Access's best practices for security enforcement, traffic filtering, and centralized management.

Question: 3

A customer is implementing Prisma Access (Managed by Strata Cloud Manager) to connect mobile users, branch locations, and business-to- business (B2B) partners to their data centers.
The solution must meet these requirements:
The mobile users must have internet filtering, data center connectivity, and remote site connectivity to the branch locations.
The branch locations must have internet filtering and data center connectivity.
The B2B partner connections must only have access to specific data center internally developed applications running on non-standard ports.
The security team must have access to manage the mobile user and access to branch locations.
The network team must have access to manage only the partner access.
Which two options will allow the engineer to support the requirements? (Choose two.)

A. Configure the CPE with Static Routes pointing to Prisma Access Infrastructure and Mobile User routes.
B. Enable eBGP for dynamic routing and configure RemoteNetworks.
C. Configure Remote Networks and define the branch IP subnets using Static Routes.

D. Enable Remote Networks Advertise Default Route.

Answer: B, C

Explanation:
Enabling eBGP for dynamic routing and configuring Remote Networks ensures seamless connectivity between branch locations, mobile users, and the data center. eBGP allows Prisma Access to dynamically exchange routes with the Customer Premises Equipment (CPE), optimizing path selection without requiring manual updates. Configuring Remote Networks and defining branch IP subnets using static routes ensures controlled and segmented routing, aligning with security policies. This setup provides proper internet filtering, data center connectivity, and restricted access for B2B partners while keeping management responsibilities aligned.

Question: 4

A customer is implementing Prisma Access (Managed by Strata Cloud Manager) to connect mobile users, branch locations, and business-to- business (B2B) partners to their data centers.
* The solution must meet these requirements:
* The mobile users must have internet filtering, data center connectivity, and remote site connectivity to the branch locations.
* The branch locations must have internet filtering and data center connectivity.
* The B2B partner connections must only have access to specific data center internally developed applications running on non-standard ports.
* The security team must have access to manage the mobile user and access to branch locations.
* The network team must have access to manage only the partner access.
Which two components can be provisioned to enable data center connectivity over the internet? (Choose two.)

A. ZTNA Connector
B. SD-WAN Connector
C. Service connections
D. Colo-Connect

Answer: C, D

Explanation:
Service connections enable secure connectivity between Prisma Access and on-premises data centers, allowing mobile users and branch locations to access internal applications. They facilitate seamless integration of internal networks with Prisma Access while maintaining security policies. Colo-Connect provides a dedicated and optimized pathway for traffic between Prisma Access and data centers, ensuring stable performance and reduced latency over the internet. Both components together support secure and efficient data center connectivity while aligning with the customer's access control and filtering requirements.

Question: 5

Which two actions can a company with Prisma Access deployed take to use the Egress IP API to automate policy rule updates when the IP addresses used by Prisma Access change? (Choose two.)

A. Configure a webhook to receive notifications of IP address changes.

B. Copy the Egress IP API Key in the service infrastructure settings.
C. Enable the Egress IP API endpoint in Prisma Access.
D. Download a client certificate to authenticate to the Egress IP API.

Answer: A, D

Explanation:
Configuring a webhook allows the company to receive real-time notifications when Prisma Access changes its egress IP addresses, ensuring that policy rules are updated automatically. Downloading a client certificate is necessary for authentication to the Egress IP API, allowing secure API access for retrieving updated IP addresses. These actions ensure that security policies remain effective without manual intervention.

Question: 6

How can an engineer verify that only the intended changes will be applied when modifying Prisma Access policy configuration in Strata Cloud Manager (SCM)?

A. Review the SCM portal for blue circular indicators next to each configuration menu item and ensure only the intended areas of configuration have this indicator.
B. Compare the candidate configuration and the most recent version under "Config Version Snapshots/
C. Select the most recent job under Operations > Push Status to view the pending changes that would apply to Prisma Access.
D. Open the push dialogue in SCM to preview all changes which would be pushed to Prisma Access.

Answer: D

Explanation:
Palo Alto Networks documentation explicitly states that the "Preview Changes" functionality within the Strata Cloud Manager (SCM) push dialogue allows engineers to review a detailed summary of all modifications that will be applied to the Prisma Access configuration before committing the changes. This is the primary and most reliable method to ensure only the intended changes are deployed.
Let's analyze why the other options are incorrect based on official documentation:
A . Review the SCM portal for blue circular indicators next to each configuration menu item and ensure only the intended areas of configuration have this indicator. While blue circular indicators might signify unsaved changes within a specific configuration section, they do not provide a comprehensive, consolidated view of all pending changes across different policy areas. This method is insufficient for verifying the entirety of the intended modifications.
B . Compare the candidate configuration and the most recent version under "Config Version Snapshots". While comparing configuration snapshots is a valuable method for understanding historical changes and potentially identifying unintended deviations after a push, it does not provide a real-time preview of the pending changes before they are applied during the current modification session

C . Select the most recent job under Operations > Push Status to view the pending changes that would apply to Prisma Access. The "Push Status" section primarily displays the status and details of completed or in-progress push operations. It does not offer a preview of the changes before a push is initiated.
Therefore, the "Preview Changes" feature within the push dialogue is the documented and recommended method for an engineer to verify that only the intended changes will be applied when modifying Prisma Access

policy configuration in Strata Cloud Manager (SCM).

Question: 7

When using the traffic replication feature in Prisma Access, where is the mirrored traffic directed for analysis?

A. Specified internal security appliance
B. Dedicated cloud storage location
C. Panorama
D. Strata Cloud Manager (SCM)

Answer: A

Explanation:
Palo Alto Networks documentation clearly states that when configuring the traffic replication feature in Prisma Access, you must specify an internal security appliance as the destination for the mirrored traffic. This appliance, typically a Palo Alto Networks next-generation firewall or a third-party security tool, is responsible for receiving and analyzing the replicated traffic for various purposes like threat analysis, troubleshooting, or compliance monitoring.
Let's analyze why the other options are incorrect based on official documentation:
B . Dedicated cloud storage location: While Prisma Access logs and other data might be stored in the cloud, the mirrored traffic for real-time analysis is directly streamed to a designated security appliance, not a passive storage location.
C . Panorama: Panorama is the centralized management system for Palo Alto Networks firewalls. While Panorama can receive logs and manage the configuration of Prisma Access, it is not the direct destination for real-time mirrored traffic intended for immediate analysis.
D . Strata Cloud Manager (SCM): Strata Cloud Manager is the platform used to configure and manage Prisma Access. It facilitates the setup of traffic replication, including specifying the destination appliance, but it does not directly receive or analyze the mirrored traffic itself.
Therefore, the mirrored traffic from the traffic replication feature in Prisma Access is directed to a specified internal security appliance for analysis.

Question: 8

When a review of devices discovered by IoT Security reveals network routers appearing multiple times with different IP addresses, which configuration will address the issue by showing only unique devices?

A. Add the duplicate entries to the ignore list in IoT Security.
B. Merge individual devices into a single device with multiple interfaces.
C. Create a custom role to merge devices with the same hostname and operating system.
D. Delete all duplicate devices, keeping only those discovered using their management IP addresses.

Answer: B

Explanation:
When network routers appear multiple times with different IP addresses in IoT Security, it is likely because they have multiple interfaces with separate IPs. Merging these entries into a single device with multiple

interfaces ensures that the system correctly identifies each router as a unique entity while maintaining visibility across all its interfaces. This approach prevents unnecessary duplicates, improves asset management, and enhances security monitoring.

Question: 9

What is the impact of selecting the “Disable Server Response Inspection” checkbox after confirming that a Security policy rule has a threat protection profile configured?

A. Only HTTP traffic from the server to the client will bypass threat inspection.

B. The threat protection profile will override the 'Disable Server Response Inspection1 only for HTTP traffic from the server to the client.

C. All traffic from the server to the client will bypass threat inspection.

D. The threat protection profile will override the 'Disable Server Response Inspection1 for all traffic from the server to the client.

Answer: C

Explanation:
Selecting the “Disable Server Response Inspection” checkbox means that traffic flowing from the server to the client will not be inspected for threats, even if a threat protection profile is applied to the Security policy rule. This setting can reduce processing overhead but may expose the network to threats embedded in server responses, such as malware or exploits.

Question: 10

A company has a Prisma Access deployment for mobile users in North America and Europe. Service connections are deployed to the data centers on these continents, and the data centers are connected by private links.
With default routing mode, which action will verify that traffic being delivered to mobile users traverses the service connection in the appropriate regions?

A. Configure BGP on the customer premises equipment (CPE) to prefer the assigned community string attribute on the mobile user prefixes in its respective Prisma Access region.

B. Configure each service connection to filter out the mobile user pool prefixes from the other region in the advertisements to the data center.

C. Configure BGP on the customer premises equipment (CPE) to prefer the MED attribute on the mobile user prefixes in its respective Prisma Access region.

D. Configure each service connection to prepend the BGP ASN five times for mobile user pool prefixes originating from the other region.

Answer: B

Explanation:
In Prisma Access's default routing mode, the service connections establish BGP sessions with the customer premises equipment (CPE) in the data centers. To ensure traffic destined for mobile users in a specific region (e.g., North America) traverses the service connection in that same region, you need to control the route

advertisements.

Filtering out the mobile user pool prefixes from the other region on each service connection achieves this by: Preventing the data center in one region from learning the specific mobile user prefixes of the other region. For example, the North American service connection would filter out the mobile user pool prefixes allocated to European users.

Ensuring that when a data center needs to send traffic to a mobile user, it will only see and use the route advertised by the service connection in the appropriate geographical region. This forces the traffic to enter the Prisma Access infrastructure through the intended regional service connection. Let's analyze why the other options are incorrect based on official documentation regarding default routing mode:

A . Configure BGP on the customer premises equipment (CPE) to prefer the assigned community string attribute on the mobile user prefixes in its respective Prisma Access region. While BGP communities can be used for influencing routing decisions, in the context of default routing mode and ensuring regional traffic flow, relying solely on the CPE to prefer community strings might not be the most robust or direct method to guarantee traffic traverses the correct regional service connection. The service connection itself needs to control the advertisement of prefixes.

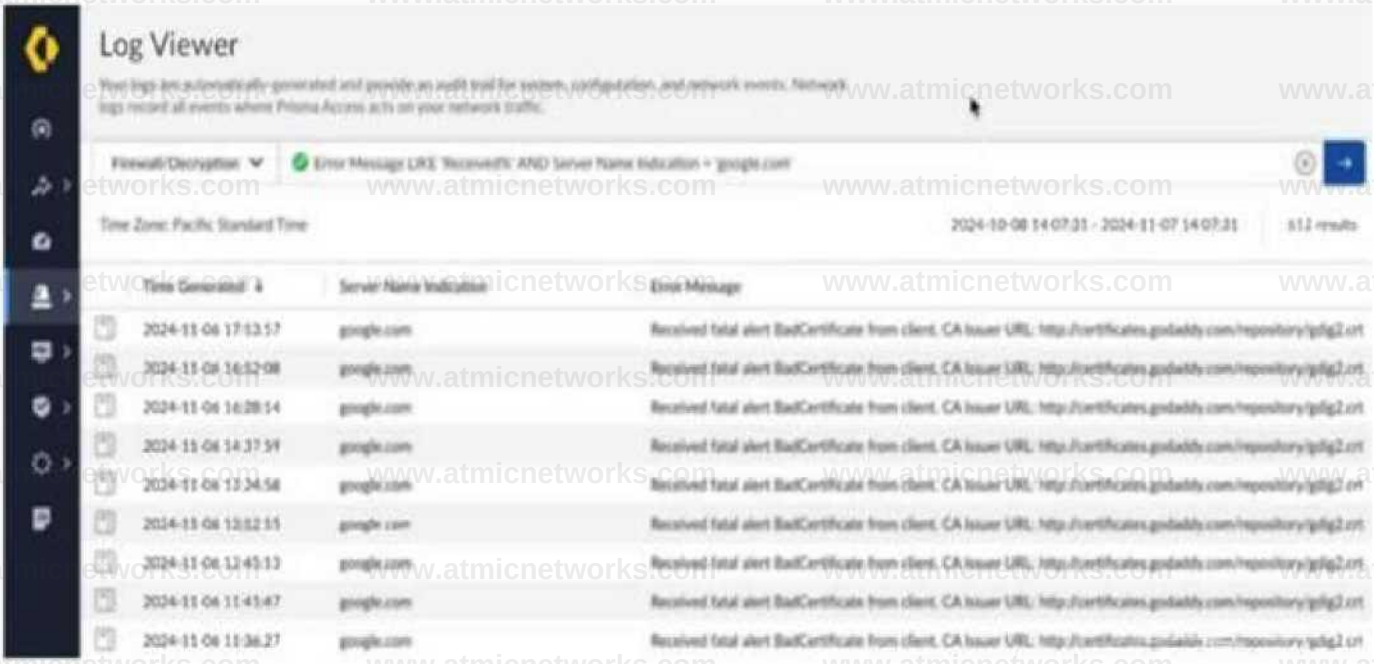
C . Configure BGP on the customer premises equipment (CPE) to prefer the MED attribute on the mobile user prefixes in its respective Prisma Access region. The BGP MED (Multi-Exit Discriminator) attribute is primarily used to influence the path selection between autonomous systems (AS) or within the same AS at different entry points. In this scenario, where service connections are advertising prefixes, filtering at the source (service connection) is a more direct and reliable way to ensure regional traffic flow than relying on the MED attribute on the CPE.

D . Configure each service connection to prepend the BGP ASN five times for mobile user pool prefixes originating from the other region. BGP AS path prepending is a mechanism to make a path less desirable. While this could influence routing, it doesn't guarantee that traffic will always take the intended regional path. Filtering provides a more definitive control over which routes are advertised and learned.

Therefore, configuring each service connection to filter out the mobile user pool prefixes from the other region in the advertisements to the data center is the verified method to ensure traffic destined for mobile users traverses the service connection in the appropriate region when using Prisma Access in default routing mode.

Question: 11

Based on the image below, which two statements describe the reason and action required to resolve the errors? (Choose two.)



A. The client is misconfigured.
B. Create a do not decrypt rule for the hostname “google.com.”
C. The server has pinned certificates.
D. Create a do not decrypt rule for the hostname “certificates.godaddy.com.”

Answer: B, C

Explanation:
The error messages indicate that Prisma Access is encountering certificate issues while attempting to decrypt traffic to "google.com." This suggests that the server has pinned certificates, meaning it does not allow man-in-the-middle (MITM) decryption by Prisma Access. Since pinned certificates prevent traffic decryption, a solution is to create a "do not decrypt" rule for the hostname "google.com." This will allow traffic to flow without triggering certificate errors while maintaining secure communication with Google's servers.

Question: 12

How can a network security team be granted full administrative access to a tenant's configuration while restricting access to other tenants by using role-based access control (RBAC) for Panorama Managed Prisma Access in a multitenant environment?

A. Create an Access Domain and restrict access to only the Device Groups and Templates for the Target Tenant.
B. Create a custom role enabling all privileges within the specific tenant's scope and assign it to the security team's user accounts.
C. Create a custom role with Device Group and Template privileges and assign it to the security team's user accounts.
D. Set the administrative accounts for the security team to the "Superuser" role.

Answer: A

Explanation:
In a Panorama Managed Prisma Access multitenant environment, Access Domains provide granular role-based access control (RBAC). By defining an Access Domain, the network security team can be granted full administrative privileges for a specific tenant's configuration while ensuring they cannot access or modify other tenants. This method enforces proper segmentation and ensures compliance with multitenant security policies.

Question: 13

An engineer has configured a Web Security rule that restricts access to certain web applications for a specific user group. During testing, the rule does not take effect as expected, and the users can still access blocked web applications.
What is a reason for this issue?

A. The rule was created with improper threat management settings.
B. The rule was created in the wrong scope, affecting only GlobalProtect users instead of all users.
C. The rule was created at a higher level in the rule hierarchy, giving priority to a lower-level rule.
D. The rule was created at a lower level in the rule hierarchy, giving priority to a higher-level rule.

Answer: D

Explanation:
Prisma Access applies security rules in a hierarchical order, where rules at higher levels take precedence over those at lower levels. If a more permissive rule is placed higher in the hierarchy, it may allow traffic before the restrictive Web Security rule is evaluated. To resolve this, the engineer should reorder the rules to ensure the restrictive Web Security rule is positioned higher in the hierarchy so it is applied before any broader or conflicting rules.

Question: 14

What will cause a connector to fail to establish a connection with the cloud gateway during the deployment of a new ZTNA Connector in a data center?

A. There is a misconfiguration in the DNS settings on the connector.
B. The connector is deployed behind a double NAT.
C. The connector is using a dynamic IP address.
D. There is a high latency in the network connection.

Answer: B

Explanation:
A ZTNA Connector requires a stable and direct connection to the cloud gateway. When the connector is deployed behind a double NAT (Network Address Translation), it can cause issues with reachability and session establishment because the cloud gateway may not be able to properly identify and communicate with the connector. Double NAT can interfere with secure tunneling, IP address resolution, and authentication mechanisms, leading to connection failures. To resolve this, the connector should be placed in a network

segment with a single NAT or a public IP assignment.

Question: 15

Which feature will fetch user and group information to verify whether a group from the Cloud Identity Engine is present on a security processing node (SPN)?

A. SASE Health Dashboard
B. User Activity Insights
C. Prisma Access Locations
D. Region Activity Insights

Answer: A

Explanation:
The SASE Health Dashboard provides visibility into user and group synchronization between the Cloud Identity Engine and the Security Processing Nodes (SPNs). It allows administrators to verify whether a group from the Cloud Identity Engine is properly fetched and available on the SPN for policy enforcement. This feature helps in troubleshooting identity-based access control issues and ensures that user group mappings are correctly applied within Prisma Access.

Question: 16

An engineer configures User-ID redistribution from an on-premises firewall connected to Prisma Access (Managed by Panorama) using a service connection. After committing the configuration, traffic from remote network connections is still not matching the correct user-based policies.
Which two configurations need to be validated? (Choose two.)

A. Ensure the Remote_Network_Template is selected when adding the User-ID Agent in Panorama. B. Confirm there is a Security policy configured in Prisma Access to allow the communication on port 5007.
C. Confirm the Collector Pre-Shared Keys match between Prisma Access and the on-premises firewall.
D. Ensure the Service_Conn_Template is selected when adding the User-ID Agent in Panorama.

Answer: A, D

Explanation:
Ensuring that the Remote_Network_Template is selected when adding the User-ID Agent in Panorama is crucial because User-ID information must be associated with the correct Remote Network configuration for policies to apply properly. Additionally, the Service_Conn_Template must be selected when adding the User-ID Agent in Panorama, as the service connection is responsible for distributing User-ID mappings between the on-premises firewall and Prisma Access. If either of these configurations is incorrect, the user information will not be properly mapped, and traffic will not match user-based policies.

Question: 17

What is the purpose of embargo rules in Prisma Access?

A. Rate-limiting connections originating from specific countries

B. Allowing traffic only from specific countries
C. Blocking connections from specific countries
D. Blocking traffic from Russia. China, and North Korea only

Answer: C

Explanation:
Embargo rules in Prisma Access are designed to block traffic from specific countries that are subject to regulatory or policy-based restrictions. These rules help organizations enforce compliance by preventing inbound and outbound connections to or from regions that may pose security risks or are restricted due to legal or geopolitical reasons. They are commonly used to align with government sanctions and corporate security policies.

Question: 18

Strata Logging Service is configured to forward logs to an external syslog server; however, a month later, there is a disruption on the syslog server.
Which action will send the missing logs to the external syslog server?

A. Configure a replay profile with the affected time range and associate it with the affected syslog server profile.
B. Delete the affected syslog server profile and create a new one.
C. Export the logs from Strata Logging Service, and then manually import them to the syslog server.
D. Configure a log filter under the syslog server profile with the affected time range.

Answer: A

Explanation:
The Strata Logging Service allows log replay, which enables resending logs that were not successfully forwarded to an external syslog server due to disruptions. By configuring a replay profile with the affected time range and associating it with the syslog server profile, Prisma Access will resend the missing logs, ensuring that all relevant data is restored in the external logging system. This approach is the most efficient and automated way to recover missing logs.

Question: 19

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

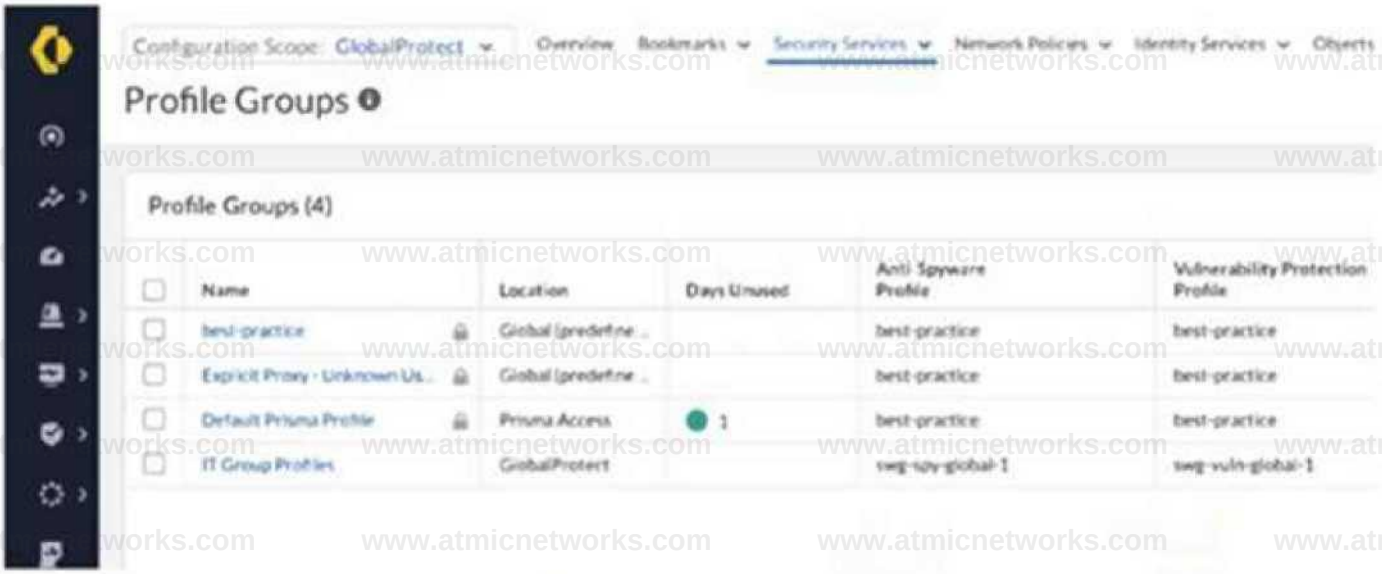
Answer: A

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: 20

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.
Therefore, the correct action is to:
Create a new Profile Group: The intern should create a new profile group within the appropriate configuration scope (likely GlobalProtect, given the task).
Configure the new Profile Group: In this new profile group, the intern can select the desired AntiSpyware 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.
Let's analyze why the other options are incorrect based on official documentation:
A . Request edit access for the GlobalProtect scope. While having the correct scope permissions is necessary for making any changes within GlobalProtect, it will not override the inherent immutability of default objects like "Default Prisma Profile." Edit access will allow the intern to create new objects and modify rules, but not directly edit the default profile group.
B . Change the configuration scope to Prisma Access and modify the profile group. The image shows that "Default Prisma Profile" has a "Location" of "Prisma Access." However, even within the Prisma Access scope, default profile groups are generally not directly editable. The issue is not the scope but the fact that it's a default object.
D . Modify the existing anti-spyware profile, because best-practice profiles cannot be removed from a group. The question is about changing the profile group, not the individual Anti-Spyware Profile.
While "best-practice" profiles might be part of default groups, the core issue is the inability to modify the default group itself. Creating a new group allows the intern to choose which Anti-Spyware Profile to include.
In summary, the fundamental principle in Palo Alto Networks management is that default objects are typically read-only to ensure a consistent and predictable baseline. To make changes, you need to create custom objects.

Question: 21

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: 22

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: 23

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: 24

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: 25

An engineer has configured IPSec tunnels for two remote network locations; however, users are experiencing intermittent connectivity issues across the tunnels.
What action will allow the engineer to receive notifications when the IPSec tunnels are down or experiencing instability?

A. Create a new notification profile specifying conditions for remote network IPSec tunnels.
B. Create a tunnel log notification rule to alert on specified remote network IPSec tunnel conditions.
C. Set up the operational health dashboard to email alerts for remote Network IPSec tunnel issues.
D. Select the IPSec tunnel monitoring and notifications checkbox when configuring the remote network IPSec tunnels.

Answer: A

Explanation:
In Prisma Access, configuring a notification profile allows engineers to receive alerts when IPSec tunnels experience downtime or instability. By defining specific conditions for remote network IPSec tunnels, the notification profile ensures that the engineer is proactively informed about tunnel failures, flapping, or degraded performance. This approach enables timely troubleshooting and minimizes disruptions for users relying on the IPSec tunnels.

Question: 26

Which two configurations must be enabled to allow App Acceleration for SaaS applications? (Choose two.)

A. Acceleration agent for the client machines
B. QoS for user traffic
C. Trusted Root CA for the CA certificate
D. Forward Trust Certificate for the CA certificate

Answer: C, D

Explanation:

To enable App Acceleration for SaaS applications in Prisma Access, the following configurations must be enabled:
Trusted Root CA for the CA certificate ensures that Prisma Access can validate and trust the SaaS application's certificates, allowing seamless inspection and acceleration of traffic without security warnings.
Forward Trust Certificate for the CA certificate enables SSL decryption for SaaS applications, allowing Prisma Access to optimize traffic and apply acceleration techniques while maintaining security policies.

Question: 27

Which two statements apply when a customer has a large branch office with employees who all arrive and log in within a five-minute time period? (Choose two.)

A. DNS results are only cached for frequently used hostnames.
B. Maximum pending TCP DNS requests is 64.
C. Maximum number of TCP DNS retries is 3.
D. DNS results are cached for 300 seconds.

Answer: B, C

Explanation:
When a large branch office experiences a high volume of employees logging in within a short time frame, the following apply:
Maximum pending TCP DNS requests is 64 – This means that Prisma Access can queue up to 64 pending DNS requests over TCP before dropping additional requests. If more requests are received simultaneously, some may fail or experience delays.
Maximum number of TCP DNS retries is 3 – If a DNS request fails over TCP, Prisma Access will attempt to retry the request up to three times before failing over to another method or returning an error.

Question: 28

Which statement applies when enabling multitenancy in Prisma Access (Managed by Panorama)?

A. Service connection licenses will be assigned only to the first tenant, and these service connections can be shared with the other tenants.
B. A single tenant cannot consist solely of mobile users or solely of remote networks.
C. Each tenant is allocated its own dedicated Prisma Access instances, with compute resources that are not shared across tenants.
D. There is flexibility to manage different tenants using separate Panoramas, which allows for better organization and management of the multiple tenants.

Answer: C

Explanation:
When multitenancy is enabled in Prisma Access (Managed by Panorama), a key characteristic is the isolation of resources between tenants. Palo Alto Networks documentation emphasizes that each tenant operates within its own logically separate Prisma Access environment. This includes dedicated compute instances, ensuring that the performance and security of one tenant are not impacted by the activities of another.

Let's analyze why the other options are incorrect based on official documentation:

A . Service connection licenses will be assigned only to the first tenant, and these service connections can be shared with the other tenants. This statement is incorrect. In a multitenant Prisma Access deployment, licenses are typically managed and allocated per tenant. While the underlying infrastructure might be shared by Palo Alto Networks, the logical resources and often the licensing

are segmented for each tenant. Sharing service connections across completely separate tenants would violate the principle of tenant isolation.

B . A single tenant cannot consist solely of mobile users or solely of remote networks. This statement is incorrect. Prisma Access multitenancy allows for flexibility in how tenants are configured. A tenant can be designed to exclusively serve mobile users, exclusively connect remote networks, or a combination of both, depending on the organizational structure and requirements.

D . There is flexibility to manage different tenants using separate Panoramas, which allows for better organization and management of the multiple tenants. While it is possible to have multiple Panorama instances managing different parts of a large infrastructure, when discussing multitenancy within a single Prisma Access instance (as implied by the question "enabling multitenancy in Prisma Access (Managed by Panorama))", all configured tenants are managed by that single Panorama instance. Managing different tenants with separate Panoramas is a different architectural consideration, not a defining characteristic of enabling multitenancy within one Prisma Access deployment managed by a specific Panorama.

Therefore, the defining characteristic of Prisma Access multitenancy (Managed by Panorama) is the allocation of dedicated Prisma Access instances and compute resources for each tenant, ensuring logical separation and resource isolation

Question: 29

A company has four branch offices between Canada Central and Canada East which use the same IPSec termination node and have QoS configured with customized bandwidth per site. An engineer wants to onboard a new branch office on the same IPSec termination node.
What is the QoS behavior for the new branch office?

A. Automatically distributed to 25% for each site
B. Unallocated until manually assigned
C. Automatically distributed to 20% for each site
D. Cannot be added to existing QoS configuration

Answer: B

Explanation:
When onboarding a new branch office to an existing IPSec termination node in Prisma Access, the QoS bandwidth is not automatically assigned. Instead, the newly added branch remains unallocated until the administrator manually assigns bandwidth within the QoS configuration settings. This ensures that customized bandwidth per site remains intact and allows for fine-tuned traffic management based on business needs.

Question: 30

A customer using Prisma Access (Managed by Panorama) wants to monitor traffic patterns across all remote networks and use Strata Logging Service to gather insights on network usage. An engineer notices that some network data is missing from the Application Command Center (ACC).

What should the engineer do to ensure complete data visibility?

A. Reconfigure the Prisma Access remote networks to log directly to Panorama instead of using Strata Logging Service.
B. Verify that the Panorama web interface has been configured to aggregate logs from both the Panorama data and RN-SPNs.
C. Enable the Use Data for Pre-Defined Reports' setting in the Logging and Reporting configuration on Panorama.
D. Ensure that log forwarding profiles are applied to all Prisma Access policies and directed to Strata Logging Service.

Answer: D

Explanation:
For complete data visibility in Prisma Access (Managed by Panorama), log forwarding profiles must be applied to all security policies to ensure that traffic logs are correctly sent to Strata Logging Service. If log forwarding is missing or misconfigured, some traffic data may not appear in the Application Command Center (ACC), leading to incomplete insights. Verifying and correctly assigning log forwarding ensures that all relevant network activity is captured and available for analysis.

Question: 31

How can a senior engineer use Strata Cloud Manager (SCM) to ensure that junior engineers are able to create compliant policies while preventing the creation of policies that may result in security gaps?

A. Use security checks under posture settings and set the action to “deny” for all checks that do not meet the compliance standards.
B. Configure role-based access controls (RBACs) for all junior engineers to limit them to creating policies in a disabled state, manually review the policies, and enable them using a senior engineer role.
C. Configure an auto tagging rule in SCM to trigger a Security policy review workflow based on a security rule tag, then instruct junior engineers to use this tag for all new Security policies.
D. Run a Best Practice Assessment (BPA) at regular intervals and manually revert any policies not meeting company compliance standards.

Answer: A

Explanation:
By using security checks under posture settings in Strata Cloud Manager (SCM), the senior engineer can enforce policy compliance standards by automatically denying any security policy that does not align with best practices. This ensures that junior engineers can create policies while preventing configurations that might introduce security gaps. This proactive approach eliminates manual oversight and enforces compliance at the

time of policy creation, reducing risk and ensuring consistent security enforcement.

Question: 32

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: 33

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: 34

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: 35

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: 36

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: 37

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: 38

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: 39

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: B, C

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: 40

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: 41

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: 42

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.
Let's analyze why the other options are incorrect based on official documentation:

A . Apply File Blocking to stop file uploads containing financial information. While File Blocking can prevent the

upload of certain file types, it is not content-aware. It cannot inspect the content of a file to determine if it contains financial information. Therefore, it's not a granular or effective solution for this specific requirement.

C . Add the ChatGPT domains using URL Filtering to block uploads containing financial information. URL Filtering controls access to specific websites or categories of websites. While you could potentially block access to ChatGPT entirely, it does not provide the capability to inspect the content being uploaded to a permitted domain and prevent the transfer of sensitive financial data.

D . Apply a vulnerability profile to stop attempts to exploit system flaws or gain unauthorized access to financial systems. Vulnerability profiles are designed to detect and prevent attempts to exploit known security vulnerabilities in systems. They are not designed to inspect the content of user uploads for sensitive data like financial information. While important for overall security, they do not directly address the requirement of preventing financial data uploads to ChatGPT.

Therefore, configuring an Enterprise DLP rule within AI Access Security is the correct and most effective method to prevent users from uploading financial information to ChatGPT by inspecting the content of the uploads.

Question: 43

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: 44

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: 45

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: 46

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: A, C

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: 47

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: 48

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: 49

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: 50

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.

Let's analyze why the other options are incorrect based on official documentation:

B . Increase the risk score for all SaaS applications to automatically block unwanted applications. Increasing the risk score for all SaaS applications, including sanctioned ones, would lead to unintended blocking and disruption of legitimate business activities. Risk score customization is intended for differentiation, not a blanket increase.

C . Build an application filter using unsanctioned SaaS as the category. While creating an application filter based on the "unsanctioned SaaS" category is a valid way to identify these applications, it directly filters based on the category itself, not the risk score. Risk score customization provides a more nuanced approach where you can define thresholds and potentially allow some low-risk activities within unsanctioned applications while blocking higher-risk ones.

D . Build an application filter using unsanctioned SaaS as the characteristic. Similar to option C, using "unsanctioned SaaS" as a characteristic in an application filter allows you to directly target these applications. However, it doesn't leverage the risk score customization feature to control access based on a graduated level of risk.

Therefore, the most effective way to use risk score customization to limit unsanctioned SaaS application usage is by lowering the risk scores of sanctioned applications and increasing the risk scores of unsanctioned ones, and then building Security policies that act upon these adjusted risk scores.