DUMPSARENA

Palo Alto Networks Security Service Edge Engineer

Palo Alto Networks SSE-Engineer

Version Demo

Total Demo Questions: 9

Total Premium Questions: 93

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Service Edge (SSE) Fundamentals	1
Topic 2, Prisma Access	74
Topic 3, Prisma Access Browser	13
Topic 4, SaaS Security	3
Topic 5, Enterprise Data Loss Prevention (DLP)	1
Topic 6, Mix Questions	1
Total	93

QUESTION NO: 1

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

A. They willexperience 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:

They will be unaffected because the plugin upgrade is transparent to users. The Cloud Services plugin is the Panorama integration component used to configure, manage, and monitor Prisma Access. Updating that management-plane plugin does not itself restart the Prisma Access data plane or intentionally tear down established user sessions and traffic flows. As a result, traffic that is already being inspected and forwarded by Prisma Access continues to use the deployed service infrastructure while the updated plugin version is installed and becomes available in Panorama. This separation is important operationally: administrators should still follow the documented upgrade workflow, confirm version compatibility, and review release notes before upgrading, but an ordinary Cloud Services plugin update is not a traffic-maintenance event that requires users' active flows to terminate. Palo Alto Networks documents plugin lifecycle and upgrade operations in the Prisma Access Panorama integration documentation, while the Prisma Access documentation describes the service as cloud-delivered infrastructure managed through Panorama. See the Prisma Access documentation portal and the Panorama documentation portal for the current plugin upgrade guidance and release-specific prerequisites.

QUESTION NO: 2

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:

SAML is the supported authentication method for mobile users when an Explicit Proxy deployment cannot use an endpoint agent. Explicit Proxy can direct web traffic from a browser to Prisma Access through PAC-file-based proxy configuration, so the authentication flow must work without a locally installed GlobalProtect component. SAML meets this requirement by using the user's browser to redirect the user to the organization's identity provider, where the user completes authentication. After the identity provider returns a successful SAML assertion, Prisma Access establishes the authenticated user session for the Explicit Proxy service.

This browser-based federation model is well suited to unmanaged devices, external networks, and mobile users because it relies on standard web redirection and an identity provider rather than endpoint software. It also allows the organization to apply its existing identity-provider controls, including multifactor authentication and conditional-access policies, before access is granted. Palo Alto Networks documents SAML authentication as the method used for Explicit Proxy mobile-user authentication, including agentless scenarios. See the Prisma Access Explicit Proxy documentation and Palo Alto Networks' Explicit Proxy authentication documentation.

QUESTION NO: 3

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: C D

Explanation:

Confirm the Collector Pre-Shared Keys match between Prisma Access and the on-premises firewall and **Ensure the Service_Conn_Template is selected when adding the User-ID Agent in Panorama** are the required validations. User-ID redistribution requires an authenticated connection between the on-premises firewall, which provides the IP-to-user mappings, and the Prisma Access infrastructure that consumes them. The collector pre-shared key is the authentication secret for this redistribution relationship. It must be identical at both ends; otherwise, the redistribution session cannot be established and Prisma Access will not receive the mappings needed to evaluate user- and group-based policy for remote-network traffic.

The receiving User-ID agent configuration must also be placed in the Prisma Access service-connection template. This template is pushed to the service-connection components that provide the path between the on-premises firewall and Prisma Access. Selecting the correct template ensures that the User-ID collector configuration, including its shared key, is present on the intended Prisma Access nodes after the template push. Once both settings are correct and committed, the redistributed mappings can be used by Prisma Access policy evaluation. Palo Alto Networks documents the service-connection template requirement in its service connection configuration documentation and describes User-ID mapping and redistribution concepts in the PAN-OS User-ID overview.

QUESTION NO: 4

All mobile users fail SAML authentication through Cloud Identity Engine after completing the Identity Provider login process. The Prisma Access portal returns an authentication failure, and the SAML URLs and certificates have already been validated. Which two log sources should the engineer correlate to identify whether the failure is in the assertion exchange or at the Identity Provider? (Choose two.)

A. Authentication logs in Strata Cloud Manager

B. Identity Provider SAML sign-in logs

C. Prisma Access URL Filtering logs

D. Remote Network IPSec tunnel logs

ANSWER: A B

Explanation:

Authentication logs in Strata Cloud Manager provide the Prisma Access and Cloud Identity Engine side of the SAML transaction, including rejected assertions and authentication processing errors. The Identity Provider SAML sign-in logs provide the corresponding IdP-side evidence, such as assertion issuance, conditional-access outcomes, and response failures.

Correlating these records by timestamp and user identifies whether the IdP generated a valid response and whether Prisma Access accepted it. Traffic logs and URL Filtering logs do not provide the SAML assertion-processing details required for this investigation.

QUESTION NO: 5

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 server has pinned certificates” identifies the underlying cause: certificate pinning is an application or service behavior in which the client expects a specific server certificate or public key. During SSL Forward Proxy decryption, Prisma Access must present a substitute certificate to the client so that it can inspect the encrypted session. A pinned-certificate validation can reject that substitute certificate even when the proxy certificate is trusted, producing connection or certificate errors. Palo Alto Networks documents certificate pinning as a situation that can require a decryption exclusion. See the Decryption Exclusions documentation for the supported approach to applications that cannot be decrypted.

“Create a do not decrypt rule for the hostname “google.com.”” is the required remediation because it excludes matching sessions from SSL decryption. Prisma Access then passes the TLS connection through without intercepting it, allowing the client and the Google host to complete their normal certificate validation directly. The rule should be scoped to the affected hostname or a narrowly defined destination wherever possible, rather than broadly disabling decryption. Palo Alto Networks decryption policy guidance describes using policy-based exceptions to bypass decryption for traffic that is incompatible with interception; see Configure Decryption Policies.

QUESTION NO: 6

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 tunnel conditions.

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:

Create a new notification profile specifying conditions for remote network IPSec tunnel conditions. In Prisma Access, notification profiles provide the mechanism for generating proactive alerts for service and connectivity events, including Remote Network IPSec tunnel status conditions. The engineer can define the applicable remote network tunnel events and configure delivery through the organization’s supported notification method, such as email. This changes tunnel visibility from a manually checked operational condition into an alert-driven workflow, so the operations team is notified when a tunnel goes down or when tunnel-health events indicate instability. The profile can be associated with the relevant Remote Network configuration, allowing the alerting scope to cover the two affected locations rather than relying on users to report loss of connectivity. This is particularly useful for intermittent symptoms because notifications provide event timing that can be correlated with tunnel status and subsequent troubleshooting data. Palo Alto Networks documents Remote Network configuration and monitoring within the Prisma Access administration documentation: Prisma Access Documentation. The official documentation search for Remote Network IPSec notification-profile guidance is available at Palo Alto Networks Documentation Search.

QUESTION NO: 7

A company is migrating from NGFW-hosted Global Protect to Prisma Access Mobile Users. The authentication method will change from LDAP with Windows Active Directory Domain Controllers to SAML with Microsoft Entra ID. After configuring and applying the SAML Authentication Profile to the Mobile Users configuration, the migrated group-based Security policies are no longer functioning. Which User-ID setting must be updated for the group-based Security policies to begin functioning?

A. Configure a redistribution profile to send user-to-group mapping from the Global Protect firewalls to Prisma Access.

B. Migrate group mapping to Cloud Identity Engine using an agent to query the Windows Active Directory Domain Controllers.

C. Modify the group mapping settings by updating the User Attributes to include " userPrincipalName. "

D. Change the SAML Authentication profile Username Modifier to %USERDOMAIN%\%USERINPUT%.

ANSWER: C

Explanation:

Modify the group mapping settings by updating the User Attributes to include `userPrincipalName`. Group-based Security policy evaluation depends on User-ID being able to associate the authenticated username with the corresponding directory user and that user's group membership. During the migration, the username supplied through the SAML assertion from Microsoft Entra ID commonly uses the user principal name format, such as `user@company.com`. The prior LDAP/Active Directory deployment may instead have mapped the identity using an Active Directory username attribute such as `sAMAccountName`. If the User-ID group-mapping profile is still correlating users only through the former attribute, Prisma Access cannot reliably resolve the SAML-authenticated identity to its mapped groups, even though the user successfully authenticates. Adding `userPrincipalName` in the User Attributes configuration aligns the group-mapping lookup with the identity format presented by Entra ID. Once the authenticated username and directory mapping use the same identity attribute, Prisma Access can determine the user's group membership and apply the migrated group-based Security policies. Palo Alto Networks describes group mapping and the user/group attributes used for User-ID correlation in its Group Mapping documentation; Microsoft documents the Entra ID user principal name attribute in its UPN guidance.

QUESTION NO: 8

How can the Prisma Access Browser (PAB) Extension extend an organization ' s web security posture to managed devices that are not connected to a VPN for browser-based access to company-sanctioned web applications?

A. It enforces consistent web access and data control policies directly within the browser on managed devices, even when they are not connected to a VPN.

B. It tunnels all endpoint traffic on unmanaged devices, ensuring all device traffic is secured.

C. It incorporates remote browser isolation (RBI) for the endpoint, running web sessions in a contained environment on any browser.

D. It optimizes network performance for browser traffic to Prisma Access for all operating systems and browsers.

ANSWER: A

Explanation:

It enforces consistent web access and data control policies directly within the browser on managed devices, even when they are not connected to a VPN. The Prisma Access Browser Extension provides a browser-layer enforcement point for supported managed-browser deployments. This allows an organization to apply its intended controls to browser sessions accessing sanctioned SaaS and web applications without requiring all traffic to traverse a GlobalProtect VPN tunnel. As a result, employees can use approved business web applications while away from the corporate network or otherwise disconnected from VPN, and the organization retains policy-based control over the browser interaction.

This approach extends security to the point where the web application is accessed: the browser. Depending on the configured policy and supported capabilities, administrators can enforce access controls and data-protection measures for browser activity, helping reduce exposure from actions such as copying, downloading, uploading, or sharing sensitive

information. The extension therefore complements network-based security rather than requiring continuous network tunneling, delivering consistent protection for managed endpoints in common SaaS-access workflows. Palo Alto Networks describes Prisma Access Browser as providing secure, controlled access through the browser and details its browser-security capabilities in its Prisma Access Browser overview and Prisma Access Browser documentation.

QUESTION NO: 9

Strata Logging Service forwards traffic logs to an external syslog server. The syslog server is unavailable for several hours and is later restored. The administrator must backfill the logs generated during the outage without changing the normal forwarding configuration. Which two actions should the administrator take? (Choose two.)

A. Create a replay profile for the outage time range.

B. Associate the replay profile with the affected syslog server profile.

C. Delete and recreate the external syslog server profile.

D. Add an outage-date filter to the normal syslog forwarding configuration.

ANSWER: A B

Explanation:

A replay profile is used to resend retained historical logs to an external destination. The profile must specify a time range that includes the syslog-server outage.

The replay profile must then be associated with the affected syslog server profile so that Strata Logging Service sends the selected historical logs to that destination. Recreating the server profile does not recover missed logs, and a log filter controls which new logs are forwarded rather than initiating historical replay.