# PaloAltoNetworks.SSE-Engineer.v2025-08-25.q18

| | |
|---|---|
| **Exam Code:** | SSE-Engineer |
| **Exam Name:** | Palo Alto Networks Security Service Edge Engineer |
| **Certification Provider:** | Palo Alto Networks |
| **Free Question Number:** | 18 |
| **Version:** | v2025-08-25 |
| **# of views:** | 130 |
| **# of Questions views:** | 180 |
| https://www.freeqas.com/qa/Palo-Alto-Networks/SSE-Engineer/PaloAltoNetworks.SSE-Engineer.v2025-08-25.q18.html | |

**NEW QUESTION: 1**
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 (LEAVE A REPLY)**
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 ofallpending 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 deviationsaftera push, it does not provide a real-time preview of thependingchanges 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 anddetails of completedorin-progresspush operations. It does not offer a preview of the changesbeforea 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).

**NEW 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: (SHOW ANSWER)**
To meet the customer's requirements,GlobalProtect and Remote Networksshould 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 asegregated and secureconnection to internal resources. It also aligns with Prisma Access's best practices forsecurity enforcement, traffic filtering, and centralized management.

**NEW QUESTION: 3**
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: (SHOW ANSWER)**
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.

**NEW QUESTION: 4**
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: (SHOW ANSWER)**
In aPanorama Managed Prisma Access multitenant environment,Access Domainsprovide granularrole- based access control (RBAC). By defining anAccess Domain, the network security team can be granted full administrative privileges for aspecific tenant's

configurationwhile ensuring theycannot access or modify other tenants. This method enforces proper segmentation andensures compliance with multitenant security policies.

**NEW QUESTION: 5**
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 (LEAVE A REPLY)**
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 thecontentof 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 importantfor 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.

**NEW QUESTION: 6**
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 (LEAVE A REPLY)**
When onboarding a new branch office to anexisting IPSec termination nodeinPrisma Access, theQoS bandwidth is not automatically assigned. Instead, the newly added branchremains unallocateduntil the administratormanually assigns bandwidthwithin theQoS configuration settings. This ensures that customized bandwidth per siteremains intact and allows forfine-tuned traffic managementbased on business needs.

**NEW QUESTION: 7**
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 (LEAVE A REPLY)**
In anExplicit Proxy deploymentwhereno agentcan be used on the endpoint,SAML (Security Assertion Markup Language)is the supported authentication method formobile users.SAMLallows authentication via anIdentity Provider (IdP)without requiring an agent on the endpoint, making it ideal for web-based authentication incloud and remote access environments. It enablesSingle Sign-On (SSO)and secure authentication without direct integration withLDAP or Kerberos, which typically require an agent or local network presence.

**NEW QUESTION: 8**
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: (SHOW ANSWER)**
The"400 Bad Request"error when attemptingSAML authenticationthrough theCloud Identity Engine (CIE)suggests amisconfiguration in the SAML metadata. This typically occurs when theendpoint URLs, certificates, or entity IDsdo not match betweenCloud Identity Engine and the IdP portal. To resolve this, verify that:
TheSAML metadatauploaded toCloud Identity Enginematches theconfiguration from the IdP.


TheACS (Assertion Consumer Service) URL, Entity ID, and certificateare correctly set.


There are no incorrect or expired certificates in theCloud Identity Engine and IdP configuration.


By ensuring theSAML metadatais properly configured inboth systems, authentication should proceed without errors.

**NEW QUESTION: 9**

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 (LEAVE A REPLY)**
TheSASE Health Dashboardprovides visibility intouser and group synchronizationbetween theCloud Identity Engine and the Security Processing Nodes (SPNs). It allows administrators to verifywhether 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 thatuser group mappings are correctly applied within Prisma Access.

**NEW QUESTION: 10**
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 (LEAVE A REPLY)**
InPrisma Access Browser (PAB), allowing access to applications while enforcingdata masking or watermarkingprovides security forBYOD (Bring Your Own Device)users without heavily impacting the user experience.Data maskingensures that sensitive information isobscured, reducing the risk of data leakage, whilewatermarkingcan deter unauthorized screenshots or data exfiltration. This approachbalances security and usability, allowing users to work efficiently while protecting corporate data.

**NEW QUESTION: 11**
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: (SHOW ANSWER)**
ForGlobalProtect with pre-logon, certificates must beinstalled in the Machine Certificate Storeto ensure that authentication occursbefore user login. This allows the GlobalProtect client to establish aVPN connection before the user logs in, enabling access to corporate resources such as domain controllers and authentication services. Usingmachine

certificatesensures secure authentication and eliminates dependency on user credentials at the pre-logon stage.

**NEW QUESTION: 12**
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 (LEAVE A REPLY)**
Strata Copilotenhances the capabilities ofPrisma Access security teamsby providingAI-powered insights and recommendationsto help resolve security issues efficiently. It analyzessecurity events, misconfigurations, and alertsand offerscontextual guidancewithrecommended next stepsfor troubleshooting and improving security posture. This assists teams inquickly identifying and addressing security challengeswithout requiring deep manual investigation.

**NEW QUESTION: 13**
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: (SHOW ANSWER)**
When terminating aPartner Interconnect-based Colo-ConnectinPrisma Access, theCustomer Premises Equipment (CPE)must supportIPSecas the overlay protocol. Prisma Access establishes secureIPSec tunnels between theColo-Connect infrastructure and the CPE, ensuringencrypted communicationand reliable connectivity.IPSecprovidessecure site-to-cloud integration, enabling customers to extend their private network securely over the Prisma Access infrastructure.

**NEW QUESTION: 14**
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 (LEAVE A REPLY)**
In amultitenant deployment, access control must be configured at theChild Tenantlevel to ensure that security administrators have full control over Security policyonly within their assigned tenantwhile restricting access to other tenants. By selectingPrisma Access & NGFW Configuration, the assigned users gain full administrative accessonly for security policy managementwithin the designated tenant, aligning with RBAC best practices for controlled access inPrisma Access Managed by Strata Cloud Manager.

**NEW QUESTION: 15**
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 (LEAVE A REPLY)**
After successfully creating aSAML authentication type and authentication profileinCloud Identity Engine
, the next step is toconfigure a corresponding SAML authentication profile in Strata Cloud Managerand link it to theCloud Identity Engine profile. This ensures thatPrisma Access (Managed by Strata Cloud Manager)can authenticate mobile users using the configured SAML identity provider (IdP), enabling seamless user authentication and access control.

**NEW QUESTION: 16**
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 (LEAVE A REPLY)**
InPrisma Access, configuring anotification profileallows engineers to receive alerts when IPSec tunnels experience downtime or instability. By definingspecific conditions for remote network IPSec tunnels, the notification profile ensures that the engineer is proactively informed abouttunnel failures, flapping, or degraded performance. This approach enables timely troubleshooting and minimizes disruptions for users relying on the IPSec tunnels.



**NEW QUESTION: 17**
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: (SHOW ANSWER)**
User mapping learned from sources other thangateway authenticationcan cause intermittent access issues if it conflicts with the expected user identity used in HIP-based policies. If the firewall is associatingthe user with an outdated or incorrect mapping, traffic may not match the intended security policies, leading todenials by the Catch-All Deny rule. If thefirewall loses user mapping due to missed HIP report checks, the user may temporarily lose access to policies that require a validHost Information Profile (HIP)match. When the VPN connection is refreshed, the HIP check is re-initiated, restoring access until the issue repeats.

**NEW QUESTION: 18**
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: (SHOW ANSWER)**
Embargo rules inPrisma Accessare designed toblock traffic from specific countriesthat are subject to regulatory or policy-based restrictions. These rules help organizations enforce compliance bypreventing inbound and outbound connectionsto or from regions that may pose security risks or arerestricted due to legal or geopolitical reasons. They are commonly used toalign with government sanctions and corporate security policies.