Exam Questions SSE-Engineer

Palo Alto Networks Security Service Edge Engineer

https://www.2passeasy.com/dumps/SSE-Engineer/

NEW QUESTION 1
A user connected to Prisma Access reports that traffic intermittently is denied after matching a Catch-All Deny rule at the bottom and bypassing HIP-based policies. Refreshing VPN connection restores the access.
What are two reasons for this behavior? (Choose two.)

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

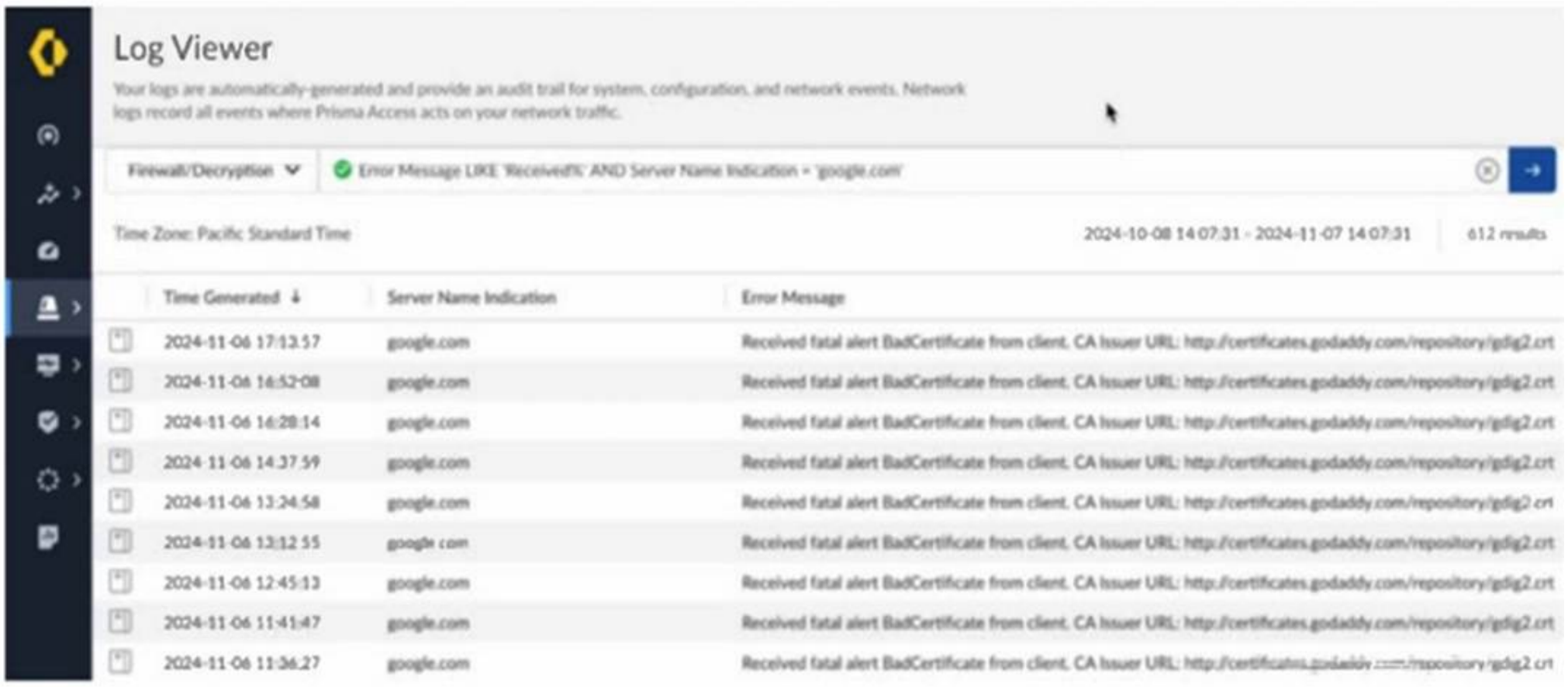
Answer: BC

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.
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: CD

NEW QUESTION 3
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.??

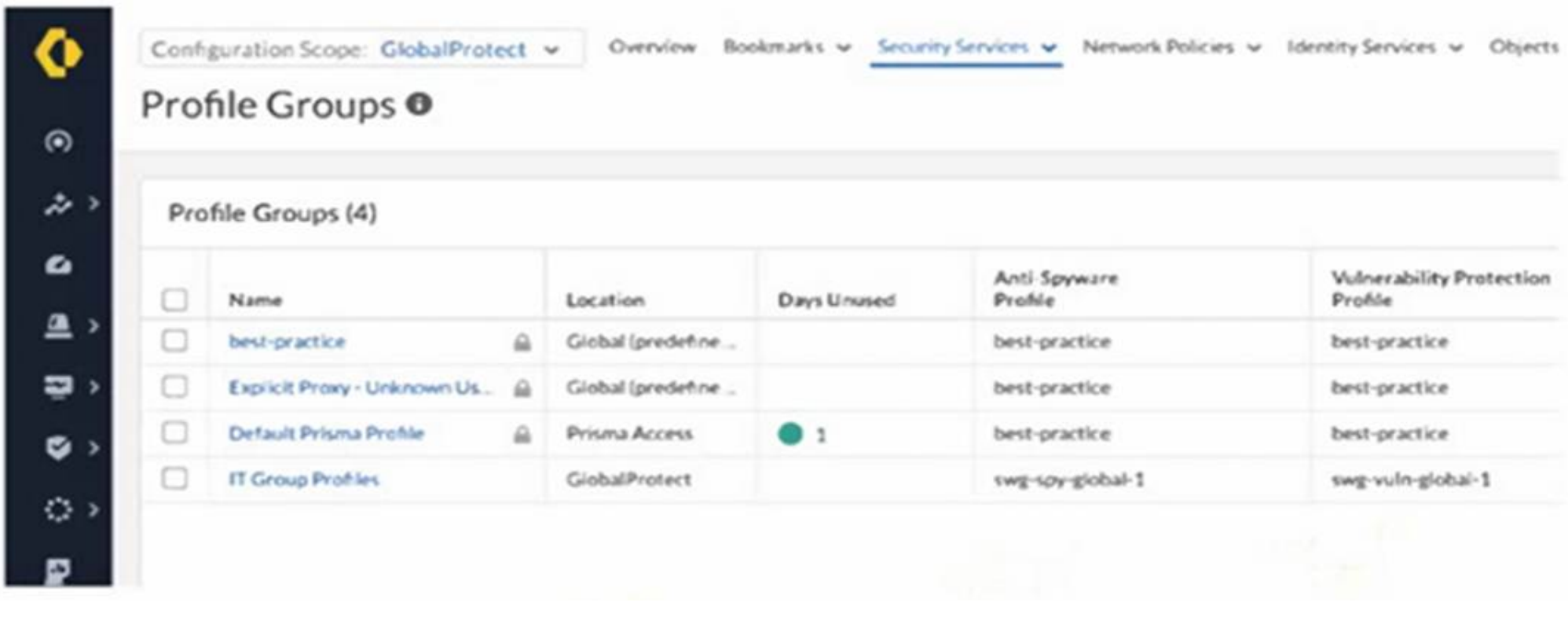
Answer: BC

NEW QUESTION 4
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

NEW QUESTION 5
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

NEW QUESTION 6
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

NEW QUESTION 7
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

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

A. Perform a full commit to Strata Cloud Manager so the Cloud Identity Engine profiles get synchronized from the application.
B. Permit the Cloud Identity Engine service account RBAC access to the mobile user folder in Strata Cloud Manager.
C. In Strata Cloud Manager, create a new authentication type of ??Cloud Identity Engine.??
D. Create a SAML authentication profile in Strata Cloud Manager and link it to the Cloud Identity Engine profile.

Answer: D

NEW QUESTION 9
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

NEW QUESTION 10
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

NEW QUESTION 10
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

NEW QUESTION 12
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

NEW QUESTION 17
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

NEW QUESTION 19
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: AD

NEW QUESTION 22
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

NEW 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

NEW QUESTION 30
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

NEW QUESTION 34
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

NEW QUESTION 35
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

NEW QUESTION 37
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

NEW QUESTION 41
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

NEW 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: AC

NEW QUESTION 48
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: BC

NEW QUESTION 52
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SSE-Engineer Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SSE-Engineer Product From:

https://www.2passeasy.com/dumps/SSE-Engineer/

Money Back Guarantee

SSE-Engineer Practice Exam Features:

* SSE-Engineer Questions and Answers Updated Frequently

* SSE-Engineer Practice Questions Verified by Expert Senior Certified Staff

* SSE-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SSE-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year