NetSec-Analyst Reliable Exam Prep & Valid NetSec-Analyst Exam Questions

2025 Latest TestSimulate NetSec-Analyst PDF Dumps and NetSec-Analyst Exam Engine Free Share: https://drive.google.com/open?id=1V7awPI29Kw3JV3Ge6wOXWDT1Nmnp5m44

To make sure your situation of passing the certificate efficiently, our NetSec-Analyst practice materials are compiled by first-rank experts. So the proficiency of our team is unquestionable. They help you review and stay on track without wasting your precious time on useless things. They handpicked what the NetSec-Analyst Study Guide usually tested in exam recent years and devoted their knowledge accumulated into these NetSec-Analyst actual tests. We are on the same team, and it is our common wish to help your realize it. So good luck!

Palo Alto Networks NetSec-Analyst Exam Syllabus Topics:

Topic	Details

Topic 1	• Management and Operations: This section of the exam measures the skills of Security Operations Professionals and covers the use of centralized management tools to maintain and monitor firewall environments. It focuses on Strata Cloud Manager, folders, snippets, automations, variables, and logging services. Candidates are also tested on using Command Center, Activity Insights, Policy Optimizer, Log Viewer, and incident-handling tools to analyze security data and improve the organization overall security posture. The goal is to validate competence in managing day-to-day firewall operations and responding to alerts effectively.
Topic 2	• Policy Creation and Application: This section of the exam measures the abilities of Firewall Administrators and focuses on creating and applying different types of policies essential to secure and manage traffic. The domain includes security policies incorporating App-ID, User-ID, and Content-ID, as well as NAT, decryption, application override, and policy-based forwarding policies. It also covers SD-WAN routing and SLA policies that influence how traffic flows across distributed environments. The section ensures professionals can design and implement policy structures that support secure, efficient network operations.
Topic 3	• Troubleshooting: This section of the exam measures the skills of Technical Support Analysts and covers the identification and resolution of configuration and operational issues. It includes troubleshooting misconfigurations, runtime errors, commit and push issues, device health concerns, and resource usage problems. This domain ensures candidates can analyze failures across management systems and on-device functions, enabling them to maintain a stable and reliable security infrastructure.
Topic 4	• Object Configuration Creation and Application: This section of the exam measures the skills of Network Security Analysts and covers the creation, configuration, and application of objects used across security environments. It focuses on building and applying various security profiles, decryption profiles, custom objects, external dynamic lists, and log forwarding profiles. Candidates are expected to understand how data security, IoT security, DoS protection, and SD-WAN profiles integrate into firewall operations. The objective of this domain is to ensure analysts can configure the foundational elements required to protect and optimize network security using Strata Cloud Manager.

Valid NetSec-Analyst Exam Questions & NetSec-Analyst Exam Online

It is a truth universally acknowledged that the exam is not easy but the related NetSec-Analyst certification is of great significance for workers in this field, I am glad to tell you that our company aims to help you to pass the NetSec-Analyst examination as well as gaining the related certification in a more efficient and simpler way. During nearly ten years, our NetSec-Analyst Exam Questions have met with warm reception and quick sale in the international market. Our NetSec-Analyst study materials are not only as reasonable priced as other makers, but also they are distinctly superior.

Palo Alto Networks Network Security Analyst Sample Questions (Q356-Q361):

NEW QUESTION # 356
A large enterprise is migrating its globally distributed Palo Alto Networks firewalls to Strata Cloud Manager (SCM). They have a complex security policy hierarchy with granular administrative access requirements. Which SCM feature is crucial for managing this complexity while adhering to a least-privilege model for their security operations team, especially when integrating with existing identity providers?

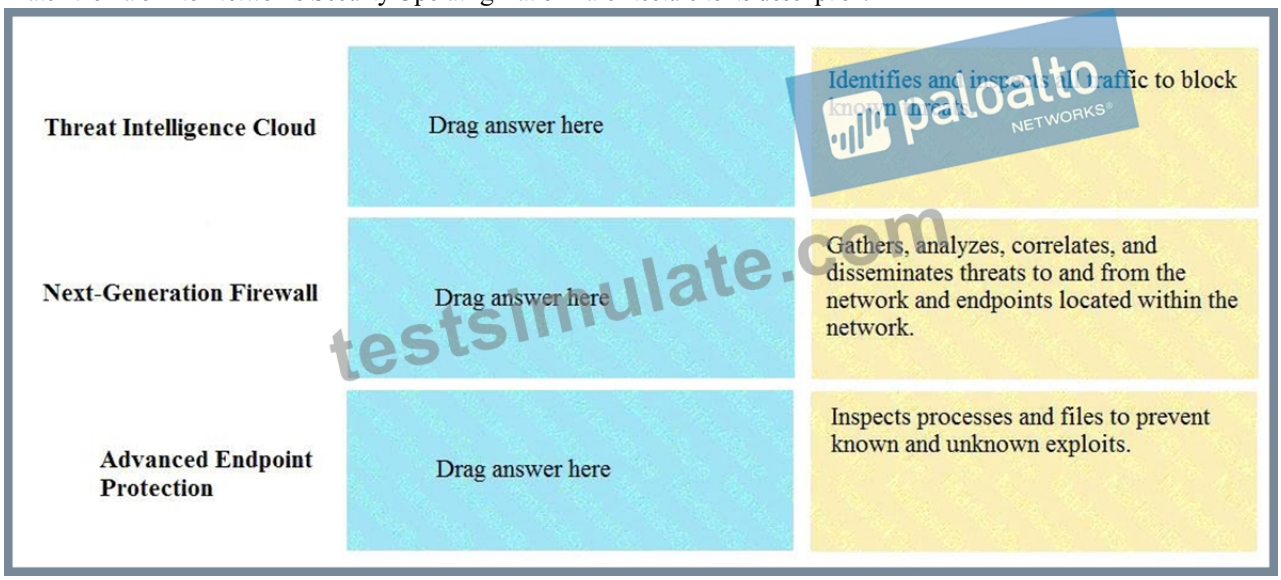
- A. Zero Touch Provisioning (ZTP)
- B. Cloud-Delivered Security Services (CDSS) subscription management
- C. Application-ID Policy Enforcement
- D. Role-Based Access Control (RBAC) with SAML/RADIUS integration
- E. SD-WAN Orchestration

Answer: D

Explanation:

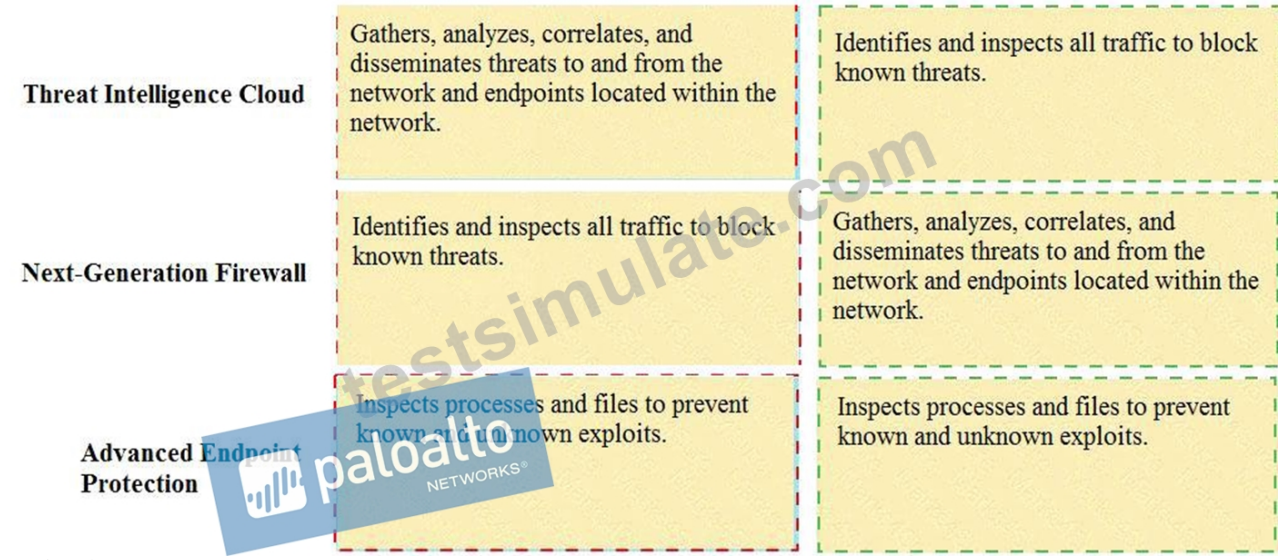
Role-Based Access Control (RBAC) in SCM allows administrators to define precise permissions for different roles (e.g., 'Policy Administrator', 'Monitor Analyst'). Integrating with existing identity providers like SAML or RADIUS ensures that user authentication and authorization are centralized and consistent with enterprise security policies, upholding the least-privilege principle. This is critical for managing complex security policy hierarchies and distributed teams.

NEW QUESTION # 357
Match the Palo Alto Networks Security Operating Platform architecture to its description.



Answer:

Explanation:



Explanation:
Threat Intelligence Cloud - Gathers, analyzes, correlates, and disseminates threats to and from the network and endpoints located within the network.
Next-Generation Firewall - Identifies and inspects all traffic to block known threats Advanced Endpoint Protection - Inspects processes and files to prevent known and unknown exploits

NEW QUESTION # 358
A Security Architect is designing a Zero Trust architecture using Palo Alto Networks firewalls. A key requirement is to ensure that all administrative access to critical infrastructure (e.g., domain controllers, internal PKI servers) is strictly controlled and logged, with any unauthorized access attempts immediately generating a 'critical' incident and being blocked. Furthermore, successful administrative access should trigger a 'low' severity alert for auditing purposes. The design must accommodate multiple zones and user groups. Which combination of Palo Alto Networks features, specifically utilizing Log Viewer and Incidents/Alerts, would

MOST effectively meet these requirements?

- A. Implement an Authentication Policy to challenge all administrative access attempts. Configure an 'Authentication Profile' with 'Action: allow' for authorized users, and a 'fall-back' action of 'deny' with 'logging enabled'. Leverage 'User-ID' for granular user-based policies. This covers access control but not necessarily distinct alert severities for allowed/denied.
- B. Create a security policy rule allowing administrative access from specific source zones/groups to destination administrative zones/servers, with 'Application: ssl, ssh, rdp', and an 'Action: allow-log'. Create a separate 'deny' rule below it for the same traffic, and set the 'Action: deny' with an 'alert profile' configured to generate critical alerts for denied connections. Successful connections will be logged, and denied connections will generate critical alerts.
- C. Configure 'Policy Based Forwarding' (PBF) to redirect all administrative traffic to a dedicated logging server, then use a SIEM to analyze logs and generate alerts based on custom rules. This offloads alerting from the firewall and Incidents page.
- D. Define dedicated security policy rules for administrative access: 1. 'Allow Admin_Access': Source Zone (Admin_Workstations), Source User Group (IT_Admins), Destination Zone (Server_Infrastructure), Destination Port (22, 3389, 443), Action: Allow, Log at Session End. Attach an 'Alert Profile' to this rule configured to generate 'low' severity alerts for 'session-start'. 2. 'Deny_Unauthorized_Admin_Access': Source Zone (Any), Destination Zone (Server_Infrastructure), Destination Port (22, 3389, 443), Action: Deny, Log at Session End. Attach an 'Alert Profile' to this rule configured to generate 'critical' severity alerts for 'session-end' (denial). Ensure rule 1 is above rule 2.
- E. Utilize 'Security Groups' and 'Dynamic Address Groups' to enforce micro-segmentation. For administrative access, create a policy allowing specific security groups to specific dynamic address groups. Rely on default logging and alerts, and review logs daily for anomalies.

Answer: D

Explanation:
Option C is the most effective and granular approach that directly addresses all specified requirements using native Palo Alto Networks features and their interaction with the Log Viewer and Incidents/Alerts page. 1. Strict Control & Logging (Allow): The first rule ('Allow_Admin_Access') explicitly defines who (IT_Admins from Admin_Workstations) can access what (Server_Infrastructure on admin ports). 'Log at Session End' ensures traffic is recorded. 2. Low Severity Alert for Successful Access: By attaching an 'Alert Profile' to the allow rule, configured for 'low' severity alerts on 'session-start', every successful administrative login attempt generates an auditable, low-severity incident. This is crucial for auditing. 3. Critical Incident for Unauthorized Access (Block): The second, broader rule ('Deny_Unauthorized_Admin_Access') acts as a catch-all for any other administrative access attempts to the critical infrastructure. By setting 'Action: Deny' and attaching an 'Alert Profile' configured for 'critical' severity alerts, any unauthorized attempt is blocked and immediately escalated as a critical incident. The order of rules (specific allow above generic deny) is critical for proper policy enforcement. Option A is less precise in separating the 'allow' and 'deny' logging/alerting requirements for different severities. Option B focuses on authentication, not the distinct logging/alerting for allowed vs. denied based on policy. Option D offloads the primary alerting functionality from the firewall, which is counter-intuitive if the Incidents and Alerts page is a key part of the solution. Option E relies on 'default' logging and manual review, which doesn't meet the 'immediately generating a critical incident' requirement.

NEW QUESTION # 359
Consider a scenario where a Palo Alto Networks firewall is configured to perform SSL Forward Proxy decryption. An internal client attempts to connect to a website with an expired certificate. Which of the following decryption profile settings would result in the connection being blocked and a corresponding log entry indicating the reason for the block?

- A. In the Decryption Profile, under 'SSL Forward Proxy', 'Block Session on Certificate Status' is unchecked, and 'Block Session on Unsupported Version' is checked.
- B. In the Decryption Profile, under 'SSL Forward Proxy', 'No Decryption' is selected, and a custom URL category for expired certificates is used in a security policy to block.
- C. In the Decryption Profile, under 'SSL Forward Proxy', 'Block Session on Certificate Status' is checked, and 'Block Session on Certificate Status' has 'Expired Certificate' selected.
- D. The firewall automatically blocks expired certificates regardless of decryption profile settings due to inherent security best practices.
- E. In the Decryption Profile, under 'SSL Forward Proxy', 'Block Session on Decryption Failure' is unchecked, and 'Block Session on Unsupported Cipher' is checked.

Answer: C

Explanation:
To block connections with expired certificates specifically, the 'Block Session on Certificate Status' option within the SSL Forward Proxy settings of the Decryption Profile must be enabled, and 'Expired Certificate' must be selected as one of the conditions to block

on. This setting directly addresses certificate validation failures during the SSL handshake. Options A and C address different failure scenarios, and D incorrectly assumes 'No Decryption' would allow such granular blocking based on certificate status.

NEW QUESTION # 360
What is a function of application tags?

- A. IP address allocations in DHCP
- B. automated referenced applications in a policy
- C. creation of new zones
- D. application prioritization

Answer: B

NEW QUESTION # 361
......

If you choose the test NetSec-Analyst certification and then buy our NetSec-Analyst study materials you will get the panacea to both get the useful certificate and spend little time. Passing the test certification can help you stand out in your colleagues and have a bright future in your career. If you buy our NetSec-Analyst Study Materials you odds to pass the test will definitely increase greatly.

P.S. Free 2025 Palo Alto Networks NetSec-Analyst dumps are available on Google Drive shared by TestSimulate: https://drive.google.com/open?id=1V7awPI29Kw3JV3Ge6wOXWDT1Nmnp5m44