Exam Sample NetSec-Analyst Online - Exam Dumps NetSec-Analyst Collection

BONUS!!! Download part of Pass4SureQuiz NetSec-Analyst dumps for free: https://drive.google.com/open?id=154CCWC71lzxTD8hl5GLDs7j1VVarOo3H

In addition, our NetSec-Analyst test prep is renowned for free renewal in the whole year. As you have experienced various kinds of exams, you must have realized that renewal is invaluable to study materials, especially to such important NetSec-Analyst exams. And there is no doubt that being acquainted with the latest trend of exams will, to a considerable extent, act as a driving force for you to pass the exams and realize your dream of living a totally different life. So if you do want to achieve your dream, buy our NetSec-Analyst practice materials.

Palo Alto Networks NetSec-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• 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 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	• 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.

Exam Dumps NetSec-Analyst Collection, NetSec-Analyst Latest Braindumps

We provide online customer service to the customers for 24 hours per day and we provide professional personnel to assist the client in the long distance online. If you have any questions and doubts about the Palo Alto Networks Network Security Analyst guide torrent we provide before or after the sale, you can contact us and we will send the customer service and the professional personnel to help you solve your issue about using NetSec-Analyst Exam Materials. If the clients have any problems or doubts about our NetSec-Analyst exam materials you can contact us by sending mails or contact us online and we will reply and solve the client's problems as quickly as we can.

Palo Alto Networks Network Security Analyst Sample Questions (Q299-Q304):

NEW QUESTION # 299
A Palo Alto Networks Network Security Analyst is tasked with optimizing security posture by decommissioning legacy, unused firewall rules. The challenge is identifying rules that genuinely have no active sessions or hit counts over an extended period (e.g., 6 months), distinguishing them from rules that might be critical but rarely triggered (e.g., a failover rule). Additionally, the analyst needs to propose a phased deprecation process to minimize risk. Which approach, integrating Command Center, Activity Insights, and Policy Optimizer, is most robust?

- A. 1. In Policy Optimizer, specifically target 'any-any' rules with low hit counts. 2. For these rules, change action to 'Alert Only' and review Command Center daily for a week. 3. If no alerts, proceed with deletion.
- B. Use Policy Optimizer's 'Rule Usage' to identify rules with zero hit count over 6 months. 2. Delete these rules. 3. Monitor Command Center for any service disruptions.
- C. 1. Utilize Command Center to view real-time session information for all active rules. 2. Identify rules with no active sessions. 3. Use Activity Insights to confirm these rules haven't had recent activity. 4. Delete the confirmed unused rules.
- D. 1. In Policy Optimizer, use the 'Security Policy Rule Optimization' dashboard to identify rules with 'Low Usage'. 2. For rules identified as 'Low Usage' and having an 'any' source, destination, or service, change the rule's action to 'No Action' (or a similar audit mode if available) with logging enabled. 3. Monitor Command Center and Activity Insights over 3-6 months for any unintended traffic disruptions or legitimate session attempts hitting the 'No Action' rule. 4. If no issues, transition the rule to 'Deny' and then eventually delete after another grace period.
- E. 1. In Activity Insights, generate a report of all 'Application Usage' and 'User Activity' over 6 months to understand baseline traffic. 2. In Policy Optimizer, use the 'Security Policy Rule Optimization' dashboard to filter for rules with low hit counts over the last 6 months. 3. For these rules, change the action to 'Deny with Logging' and observe Command Center for new 'deny' logs. 4. If no legitimate denies, decommission the rule.

Answer: D

Explanation:
This is a comprehensive, risk-averse approach. Policy Optimizer's 'Security Policy Rule Optimization' is the core tool for identifying 'Low Usage' rules. The key differentiator here is the proposed phased deprecation: changing the rule to an 'audit mode' (like 'No Action' or setting an action that logs but doesn't block) first, and monitoring Command Center for real-time impact and Activity Insights for long-term trends. This allows for validation that the rule is truly unused without immediately causing an outage, especially

for rarely-triggered but critical rules (like failover). Only after a prolonged monitoring period and confirmation of no impact should the rule be moved to 'Deny' and then finally deleted, minimizing risk.

NEW QUESTION # 300
An organization is performing a disaster recovery test for its Palo Alto Networks firewall infrastructure managed by Strata Cloud Manager (SCM). The test scenario involves simulating a complete loss of the primary data center where some physical firewalls reside. The goal is to quickly provision new firewalls in a secondary data center, apply the latest configurations and policies from SCM, and verify operational status with minimal manual intervention. Which SCM features and principles would be critical for a successful, rapid recovery in this context? (Select all that apply)

- A. Real-time visibility and monitoring dashboards to confirm successful firewall re-integration and traffic flow.
- B. Zero Touch Provisioning (ZTP) to automatically onboard new firewalls upon network connectivity.
- C. Automated software upgrade scheduling for future maintenance cycles.
- D. API integration with orchestration tools to trigger firewall provisioning and policy pushes.
- E. SCM's centralized policy and object repository ensuring all configurations are backed up and accessible.

Answer: A,B,D,E

Explanation:
A successful rapid disaster recovery relies on several SCM capabilities. -A. Zero Touch Provisioning (ZTP): New firewalls can automatically pull their initial configuration from SCM as soon as they connect to the network, eliminating manual onboarding. - B. SCM's centralized policy and object repository: All device group configurations, shared policies, and objects are stored in SCM, acting as the authoritative backup source for configurations. - D. API integration with orchestration tools: For rapid and automated recovery, external orchestration tools can use SCM's API to initiate ZTP for new devices, assign them to device groups, and trigger policy pushes. - E. Real-time visibility and monitoring dashboards: After provisioning and policy application, SCM's monitoring capabilities provide immediate feedback on the operational status of the new firewalls, traffic flow, and security events, confirming the success of the recovery. - C is less critical for rapid recovery and more for ongoing operations.

NEW QUESTION # 301
The firewall sends employees an application block page when they try to access Youtube.
Which Security policy rule is blocking the youtube application?

- A. Deny Google
- B. intrazone-default
- C. interzone-default
- D. allowed-security services

Answer: C

NEW QUESTION # 302
An organization relies heavily on cloud-based Software as a Service (SaaS) applications. They need to implement a security policy that allows access to approved SaaS applications (e.g., Office 365, Box) but strictly blocks all other SaaS applications, and also prevents any shadow IT usage. Furthermore, for approved SaaS applications, the organization wants to apply specific content inspection profiles for data loss prevention and malware prevention. Which combination of Security Policy rules and features would be the most robust and maintainable?

- A. Rule 1 (Allow): Source: Internal, Destination: Untrust, Application Filter: 'SaaS', Action: allow, Profiles: Data Filtering, Antivirus. Rule 2 (Deny): Source: Internal, Destination: Untrust, Application: any, Action: deny.
- B. Rule 1 (Allow): Source: Internal, Destination: Untrust, Application: office365-base, box-base, Service: tcp/443, Action: allow, Profiles: URL Filtering (allow approved SaaS URLs). Rule 2 (Deny): Source: Internal, Destination: Untrust, Application: any, Service: tcp/443, Action: deny.
- C. Rule 1 (Allow): Source: Internal, Destination: Untrust, Application: office365-base, box-base, Service: application-default, Action: allow, Profiles: Data Filtering, Antivirus. Rule 2 (Deny): Source: Internal, Destination: Untrust, Application: any, Service: any, Action: deny.
- D. Rule 1 (Allow): Source: Internal, Destination: Untrust, Application Group: 'Approved_SaaS_Applications' (with App-IDs for Office 365, Box etc.), Service: application-default, Action: allow, Profiles: Data Filtering, Antivirus, WildFire, Spyware. Rule 2 (Deny): Source: Internal, Destination: Untrust, Application Group: 'Unknown_SaaS_Applications' (using App-ID

filters), Service: application-default, Action: deny. Rule 3 (Final Deny): Source: Internal, Destination: Untrust, Application: any, Service: any, Action: deny.

- E. Rule 1 (Allow): Source: Internal, Destination: Untrust, Application Filter: 'Approved_SaaS_Apps' (custom filter group), Service: application-default, Action: allow, Profiles: Data Filtering, Antivirus, Vulnerability Protection, URL Filtering (block unknown/unrated). Rule 2 (Deny): Source: Internal, Destination: Untrust, Application: any, Service: application-default, Action: deny.

Answer: E

Explanation:
Option C is the most robust and maintainable. Creating a custom Application Filter Group ('Approved_SaaS_Apps') allows for easy management of allowed SaaS applications. Applying comprehensive security profiles (Data Filtering, Antivirus, Vulnerability Protection, URL Filtering to block unknown/unrated) to this allowed traffic ensures deep inspection and protection. The subsequent 'deny any' rule acts as a catch- all to block all other unwanted traffic, including unapproved SaaS and shadow IT. Option E is also good but creates unnecessary complexity with an 'Unknown_SaaS_Applications' group when a simple final 'deny any' is sufficient after allowing known good. Option A and D are less granular and might miss some SaaS traffic. Option B's 'SaaS' filter might include unapproved SaaS, defeating the purpose of strict control.

NEW QUESTION # 303
A secure healthcare network leverages Palo Alto Networks NGFWs to protect critical medical IoT devices (IoMT) like infusion pumps and patient monitors. These devices communicate using proprietary protocols over TCP. The security team has identified that some of these devices are attempting to establish undocumented SSH connections to external IP addresses, likely due to a compromise. The challenge is that the NGFW's 'Application-ID' correctly identifies the proprietary IoMT application, but it also identifies the rogue SSH connection from the same device . How can the security policy, leveraging IoT security profiles, be configured to allow the legitimate IoMT proprietary application while blocking the specific SSH connection from the compromised device without disrupting essential medical operations?

- A. Configure an 'IoT Security Profile' with 'Application Function Filtering' to disable all functions of the proprietary IoMT application, effectively blocking all communication.
- B. Utilize 'Application Filters' to create a 'Permitted-IoMT-Apps' group including only the proprietary IoMT application. Create a 'Security Policy' rule allowing only this 'Permitted-IoMT-Apps' group from the IoMT device group, effectively denying other applications like SSH.
- C. Implement 'Application Override' for the proprietary IoMT application's port, forcing all traffic on that port to be identified as the legitimate IoMT app, thereby preventing SSH from being identified.
- D. Create a 'Security Policy' rule with 'Source: Compromised-IoMT-Device-Group', 'Destination: Any', 'Application: ssh', 'Action: Deny'. Place this rule above the general 'Allow' rule for IoMT devices.
- E. Apply an 'Anti-Spyware' profile to the IoMT security policy with a custom signature for the specific SSH traffic pattern observed from the compromised device.

Answer: D

Explanation:
Option A is the most effective and precise solution. Palo Alto Networks' 'Application-ID' works by identifying applications regardless of port. If both the proprietary IoMT app and SSH are identified from the same device, the most direct way to block SSH while allowing the legitimate app is to create a specific 'deny' rule for SSH, targeted at the compromised device (or device group), and place it higher in the rulebase than any 'allow' rule for that device/group. Since firewall rules are processed top-down, the deny for SSH will be hit first. Option B is incorrect as it would block all legitimate IoMT functions. Option C (Anti-Spyware with custom signature) is a reactive measure for known threats; policy-based blocking is more direct for application control. Option D (Application Override) is a misapplication; it would force all traffic on the IoMT port to be seen as the IoMT app, potentially masking the rogue SSH if it uses the same port, or preventing accurate identification if SSH uses a different port. Application-ID is already correctly identifying both. Option E is a good general practice for 'least privilege' (allowing only known applications), but Option A specifically addresses the immediate need to block the identified SSH from the compromised device without affecting the legitimate IoMT app.

NEW QUESTION # 304
.....

during your review, you can take joy and challenge theNetSec-Analyst Exam may bring you by the help of our NetSec-Analyst guide braindumps. You will be surprised by the high-effective of our NetSec-Analyst study guide!

Exam Dumps NetSec-Analyst Collection: https://www.pass4surequiz.com/NetSec-Analyst-exam-quiz.html