NetSec-Analyst考古題更新 & NetSec-Analyst資料

P.S. KaoGuTi在Google Drive上分享了免費的2026 Palo Alto Networks NetSec-Analyst考試題庫：https://drive.google.com/open?id=13_qZwES_PHlikKkmZsWBmsvptglZB6ba

NetSec-Analyst認證考試是一個很難的考試。但是即使這個考試很難，報名參加考試的人也很多。如果要說為什麼，那當然是因為NetSec-Analyst考試是一個非常重要的考試。對IT職員來說，沒有取得這個資格那麼會對工作帶來不好的影響。這個考試的認證資格可以給你的工作帶來很多有益的幫助，也可以幫助你晉升。總之這是一個可以給你的職業生涯帶來重大影響的考試。这么重要的考试，你也想参加吧。

Palo Alto Networks NetSec-Analyst 考試大綱：

主題	簡介
主題 1	• 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.
主題 2	• 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.

主題 3	• 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.
主題 4	• 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.

Palo Alto Networks NetSec-Analyst資料 - NetSec-Analyst題庫下載

KaoGuTi的NetSec-Analyst考古題的命中率很高，可以幫助大家一次通過考試。這是經過很多考生證明過的事實。所以不用擔心這個考古題的品質，這絕對是最值得你信賴的考試資料。如果你還是不相信的話，那就趕快自己來體驗一下吧。你絕对會相信我的话的。

最新的 Network Security Administrator NetSec-Analyst 免費考試真題 (Q150-Q155):

問題 #150

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, 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.
- B. 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.
- C. 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.
- D. 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.
- E. 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.

答案：A

解題說明：
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.

問題 #151

An administrator wants to reference the same address object in Security policies on 100 Panorama managed firewalls, across 10 device groups and five templates.

Which configuration action should the administrator take when creating the address object?

- A. Ensure that the Shared option is checked.
- B. Ensure that the Shared option is cleared.
- C. Ensure that Disable Override is cleared.
- D. Tag the address object with the Global tag.

答案：A

解題說明：

To reference the same address object in Security policies on 100 Panorama-managed firewalls, across 10 device groups and five templates, the administrator should ensure that the Shared option is checked when creating the address object. This option allows the administrator to create a shared address object that is available to all device groups and templates on Panorama. The shared address object can then be used in multiple firewall policy rules, filters, and other functions1. This reduces the complexity and duplication of managing address objects across multiple firewalls2. References: Address Objects, Create a Shared Address Object, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

問題 #152

Consider the following Python script designed to generate an External Dynamic List for Palo Alto Networks firewalls. The script pulls data from an API and formats it. If an administrator notices that their firewall EDL is always empty, despite the API returning data, what could be the issue with the generated file or its handling by the firewall?

- A. The 'Repeat' interval on the firewall's EDL configuration is set to 'Never'.
- B. The script is not accessible via HTTP/HTTPS at the configured EDL source URL.
- C. The firewall does not support the Python script's execution environment.
- D. The API rate limits the script's requests, causing intermittent failures.
- E. The output file does not contain a new line character after each entry, or the file is not served with the correct MIME type (e.g.,

答案：E

解題說明：

If the EDL is consistently empty, it implies the firewall is fetching something but isn't finding valid entries. Option B (Correct): Palo Alto Networks firewalls are strict about EDL file formatting. Each entry must be on a new line. If entries are concatenated or the file is not served as plain text, the firewall will likely parse it as empty or invalid. This is a common pitfall when scripting EDL generation. Option A would result in a 'connection refused' or 'file not found' error, not an empty list. Option C is irrelevant; the script runs on the web server, not the firewall. Option D would mean the EDL never updates at all, not that it's empty after updates. Option E would cause intermittent failures, not consistently empty lists.

問題 #153

Which three filter columns are available when setting up an Application Filter? (Choose three.)

- A. Subcategory
- B. Parent App
- C. Risk
- D. Category
- E. Standard Ports

答案：A,C,D

解題說明：

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-application-filters

問題 #154
A website is unexpectedly allowed due to miscategorization.
What are two way-s to resolve this issue for a proper response? (Choose two.)

- A. Create a URL category and assign the affected URL.Add a Security policy with a URL category qualifier of the custom URL category below the original policy. Set the policy action to Deny.
- B. Identify the URL category being assigned to the website.Edit the active URL Filtering profile and update that category's site access settings to block.
- C. Create a URL category and assign the affected URL.Update the active URL Filtering profile site access setting for the custom URL category to block.
- D. Review the categorization of the website on https://urlfiltering.paloaltonetworks.com.Submit for "request change*, identifying the appropriate categorization, and wait for confirmation before testing again.

答案：A,D

問題 #155
......

如果你不知道如何更有效的通過考試，我給你一個建議是選擇一個良好的培訓網站，這樣可以起到事半功倍的效果。我們KaoGuT網站始終致力於為廣大考生提供全部真實的 Palo Alto Networks的NetSec-Analyst認證的考試培訓資料，KaoGuTi Palo Alto Networks的NetSec-Analyst認證考試考古題軟體供應商授權的產品，覆蓋率廣，可以為你節省大量的時間和精力。