NetSec-Analyst Frequent Updates & NetSec-Analyst Test Engine

DOWNLOAD the newest ITPassLeader NetSec-Analyst PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1M5UboHf-DxKh-KyFzhwWN_0voP1gcCog

If you purchase Palo Alto Networks NetSec-Analyst exam questions and review it as required, you will be bound to successfully pass the exam. And if you still don't believe what we are saying, you can log on our platform right now and get a trial version of Palo Alto Networks Network Security Analyst NetSec-Analyst study engine for free to experience the magic of it.

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	• 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	• 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 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.

NetSec-Analyst Test Engine - Reliable NetSec-Analyst Exam Voucher

ITPassLeader is a specialized IT certification exam training website which provide you the targeted exercises and current exams. We focus on the popular Palo Alto Networks Certification NetSec-Analyst Exam and has studied out the latest training programs about Palo Alto Networks certification NetSec-Analyst exam, which can meet the needs of many people. Palo Alto Networks NetSec-Analyst certification is a reference of many well-known IT companies to hire IT employee. So this certification exam is very popular now. ITPassLeader is also recognized and relied by many people. ITPassLeader can help a lot of people achieve their dream. If you choose ITPassLeader, but you do not successfully pass the examination, ITPassLeader will give you a full refund.

Palo Alto Networks Network Security Analyst Sample Questions (Q114-Q119):

NEW QUESTION # 114
What is the default action for the SYN Flood option within the DoS Protection profile?

- A. Random Early Drop
- B. Reset-client
- C. Sinkhole
- D. Alert

Answer: A

Explanation:
Random Early Drop -The firewall uses an algorithm to progressively start dropping that type of packet. If the attack continues, the higher the incoming cps rate (above the Activate Rate) gets, the more packets the firewall drops. .. (https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/dos-protection-against-flooding-of-new-sessions/configure-dos-protection-against-flooding-of-new-sessions)

NEW QUESTION # 115
You are tasked with analyzing the long-term resource usage trends of a Palo Alto Networks firewall to justify a hardware upgrade. You need to gather specific metrics over the past year, including average and peak session counts, CPU utilization (data plane and management plane), and throughput. Which of the following methods provides the MOST comprehensive and historical data for this purpose, assuming the firewall is managed by Panorama?

- A. Periodically log into the firewall CLI and run show running resource-monitor all, then manually compile the data into a spreadsheet.
- B. Utilize Panorama's 'ACC' (Application Command Center) for 'GlobalProtect', 'Threat', and 'Traffic' monitoring, as these indirectly reflect resource usage.
- C. Configure SNMP traps on the firewall to send resource utilization data to an external monitoring system with long-term data retention capabilities.
- D. Leverage Panorama's 'Managed Devices' tab, navigate to the specific firewall, and view 'System' and 'Network' dashboards for historical graphs and data summaries.
- E. Extract 'Resource Monitor' reports directly from the firewall's GUI (Monitor > Reports > Resource Monitor) for various timeframes.

Answer: C

Explanation:

For long-term, comprehensive, and historical resource usage analysis to justify an upgrade, SNMP with an external monitoring system (Option D) is the most effective. While Panorama (Option C) provides some historical data, its native retention for detailed resource metrics like specific CPU core utilization or granular session counts over a year is often limited by its logging and reporting capacity and configured data retention periods. A dedicated SNMP monitoring system (e.g., SolarWinds, PRTG, Zabbix, Grafana/Prometheus) can collect and store these metrics with much greater granularity and for extended periods, allowing for custom reporting, trend analysis, and predictive modeling for capacity planning. Options A and B are manual and limited in scope/history. Option E focuses on traffic/threats, not direct resource utilization trends for hardware sizing.

NEW QUESTION # 116
A network architect is designing a decryption strategy for outbound traffic, including advanced threat protection. The requirement states that traffic to known malicious sites (categorized by a custom URL category 'Malicious_Domains') must be blocked immediately without decryption, whereas traffic to cloud storage services (e.g., Google Drive, Dropbox) must be decrypted for DLP inspection. All other internet-bound TLS traffic should be decrypted by default, with an emphasis on blocking connections that utilize deprecated SSL/TLS versions or weak ciphers. Assume the following objects exist: 'DLP_Decryption_Profile' (Forward Proxy, strong cipher/protocol requirements), 'No_Decryption_Profile', and 'Block_Profile' (a security profile with action block).

- A. Rule 1: Source: Any, Destination: Malicious_Domains, Service: application-default, Action: Deny. Rule 2: Source: Any, Destination: Any, Service: application- default, Action: Allow, Decryption Profile: DLP_Decryption_Profile. Rule 3: Source: Any, Destination: cloud-storage-apps, Service: application-default, Action: Allow, Decryption Profile: DLP_Decryption_Profile.
- B. Rule 1: Source: Any, Destination: Malicious_Domains, Service: application-default, Action: Deny. Rule 2: Source: Any, Destination: cloud-storage-apps, Service: application-default, Action: Allow, Decryption Profile: No_Decryption_Profile. Rule 3: Source: Any, Destination: Any, Service: application-default, Action: Allow, Decryption Profile:
- C. Rule 1: Source: Any, Destination: Malicious_Domains, Service: application-default, Action: Deny. Rule 2: Source: Any, Destination: cloud-storage-apps, Service: application-default, Action: Allow, Decryption Profile: DLP_Decryption_Profile. Rule 3: Source: Any, Destination: Any, Service: application-default, Action: Allow, Decryption Profile: DLP_Decryption_Profile.
- D. Rule 1: Source: Any, Destination: cloud-storage-apps, Service: application-default, Action: Allow, Decryption Profile: DLP_Decryption_Profile. Rule 2: Source: Any, Destination: Malicious_Domains, Service: application-default, Action: Deny. Rule 3: Source: Any, Destination: Any, Service: application-default, Action: Allow, Decryption Profile: DLP_Decryption_Profile.
- E. Rule 1: Source: Any, Destination: cloud-storage-apps, Service: ssl, Action: Allow, Decryption Profile: DLP_Decryption_Profile. Rule 2: Source: Any, Destination: Malicious_Domains, Service: ssl, Action: Deny. Rule 3: Source: Any, Destination: Any, Service: ssl, Action: Allow, Decryption Profile: DLP_Decryption_Profile.

Answer: C

Explanation:
The order of security policy rules is critical. First, traffic to known malicious sites should be explicitly denied before any decryption attempts, to prevent potential compromises. Second, specific traffic requiring decryption (cloud storage for DLP) should be handled. Finally, a general rule applies the default decryption policy to all other traffic. Option A correctly sequences these requirements: Block malicious first, then decrypt specific applications, then decrypt general traffic. Using 'application-default' is appropriate for most scenarios as it identifies the actual application.

NEW QUESTION # 117
Which three types of entries can be excluded from an external dynamic list (EDL)? (Choose three.)

- A. URLs
- B. User-ID
- C. IP addresses
- D. Applications
- E. Domains

Answer: A,C,E

Explanation:
Three types of entries that can be excluded from an external dynamic list (EDL) are IP addresses, domains, and URLs. An EDL is a text file that is hosted on an external web server and contains a list of objects, such as IP addresses, URLs, domains, International Mobile Equipment Identities (IMEIs), or International Mobile Subscriber Identities (IMSIs) that the firewall can import and use in

policy rules. You can exclude entries from an EDL to prevent the firewall from enforcing policy on those entries. For example, you can exclude benign domains that applications use for background traffic from Authentication policy1. To exclude entries from an EDL, you need to:
Select the EDL on the firewall and click Manual Exceptions.
Add the entries that you want to exclude in the Manual Exceptions list. The entries must match the type and format of the EDL. For example, if the EDL contains IP addresses, you can only exclude IP addresses.
Click OK to save the changes. The firewall will not enforce policy on the excluded entries.

NEW QUESTION # 118
A Palo Alto Networks firewall is configured with User-ID and integrated with Active Directory. The network team reports that users from the 'Guest Wi-Fi' network are occasionally accessing internal resources. The current security policy allows 'Guest_Wi-Fi' users only to specific internet sites. Investigation reveals that the Guest Wi-Fi SSID is configured to assign IPs from a different subnet than the corporate network, but the User-ID mapping is still showing internal corporate users mapped to some Guest Wi-Fi IPs due to cached logins or session sharing. How would you prevent 'Guest_Wi-Fi' users, regardless of their User-ID mapping, from accessing internal resources while maintaining their internet access?

- A. Create a new Security Policy rule with Source Zone: Guest_Zone, Source User: any, Destination Zone: Internal_Zone, Action: deny. Place this rule above all other internal access rules.
- B. Configure a User-ID exclusion list for the Guest_Wi-Fi subnet to prevent any User-ID mappings for those IPs, then create a deny rule for Guest_Zone to Internal Zone.
- C. Modify the existing rules for 'Guest_Wi-Fi' internet access by adding Destination Zone: Untrust and ensuring no rules allow Guest_Wi-Fi to Internal_Zone. Clear User-ID cache periodically.
- D. Implement an explicit Policy-Based Forwarding (PBF) rule for the Guest_Wi-Fi subnet to route all traffic directly to the internet, bypassing security policy evaluation for internal destinations.
- E. Create a new Security Policy rule with Source Zone: Guest_Zone, Source Address: Guest_Wi-Fi_Subnet, Source User: any, Destination Zone: Internal_Zone, Action: deny. Place this rule with the highest priority.

Answer: E

Explanation:
Option C is the most direct and effective solution. By creating a deny rule that specifies the 'Guest_Zone' as the source zone and the 'Guest_Wi-Fi_Subnet' as the source address, you explicitly block any traffic originating from that subnet from reaching the 'Internal_Zone', irrespective of any potentially incorrect User-ID mappings. Placing this rule with the highest priority ensures it's evaluated first. User-ID cache issues or session sharing can lead to incorrect user mappings, so relying solely on User-ID in this specific cross-zone scenario can be problematic. Option D could work but is more complex than needed for this specific problem. Option E would bypass security policies entirely and isn't a policy-based solution. Option A is less precise as it doesn't explicitly use the source address. Option B relies on clearing cache, which is reactive and not a preventative policy.

NEW QUESTION # 119
.....

Free

- Quiz 2026 Palo Alto Networks NetSec-Analyst: Palo Alto Networks Network Security Analyst Marvelous Frequent Updates □ Download ✔ NetSec-Analyst □✔□ for free by simply searching on 【 www.practicevce.com 】 □Latest NetSec-Analyst Braindumps Sheet
- Latest NetSec-Analyst Braindumps Sheet □ NetSec-Analyst Reliable Exam Papers □ NetSec-Analyst Reliable Dumps Ebook □ The page for free download of 【 NetSec-Analyst 】 on ➤ www.pdfvce.com □ will open immediately □NetSec-Analyst Test Price
- NetSec-Analyst Reliable Dumps Ebook □ NetSec-Analyst Real Sheets □ NetSec-Analyst Valid Dumps Free □ Download [NetSec-Analyst] for free by simply searching on （ www.examcollectionpass.com ） □Latest NetSec-Analyst Braindumps Sheet
- Quiz 2026 NetSec-Analyst: Palo Alto Networks Network Security Analyst Marvelous Frequent Updates □ Search for （ NetSec-Analyst ） and download it for free on ➽ www.pdfvce.com □ website □NetSec-Analyst Reliable Exam Preparation
- Free PDF 2026 Pass-Sure Palo Alto Networks NetSec-Analyst: Palo Alto Networks Network Security Analyst Frequent Updates □ Open website ☀ www.vce4dumps.com □☀□ and search for ➡ NetSec-Analyst □□□ for free download □ □Latest NetSec-Analyst Learning Material
- NetSec-Analyst Valid Dumps Free □ Download NetSec-Analyst Demo □ NetSec-Analyst Latest Study Questions □ Search on { www.pdfvce.com } for ➡ NetSec-Analyst □□□ to obtain exam materials for free download □NetSec-Analyst Vce Files
- NetSec-Analyst Vce Files □ NetSec-Analyst Valid Exam Registration □ Download NetSec-Analyst Demo □ Search for □ NetSec-Analyst □ on ➤ www.prepawaypdf.com □ immediately to obtain a free download □NetSec-Analyst New Braindumps
- owners111.com, study.stcs.edu.np, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, saintraphaelcareerinstitute.net, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that ITPassLeader NetSec-Analyst dumps now are free: https://drive.google.com/open?id=1M5UboHf-DxKh-KyFzhwWN_0voP1gcCog