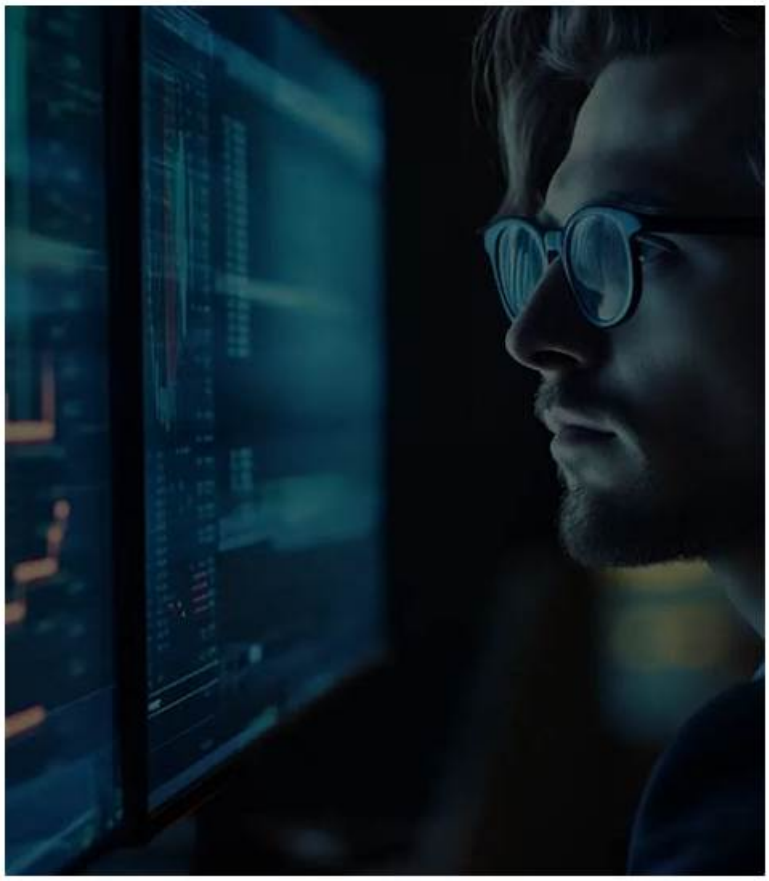
Latest NetSec-Analyst Study Tool Offer You The Best New Braindumps Free | Palo Alto Networks Network Security Analyst



In order to have better life, attending certification exams and obtaining certifications will be essential on the path to success. NetSec-Analyst latest test cram sheet will help you achieve your goal. Only if you receive the certificate the companies require you can have the opportunities for raising-salary and promotion. Thousands of companies think highly of this certification. You will be popular if you pass exam with NetSec-Analyst Latest Test Cram sheet.

Once you learn all NetSec-Analyst questions and answers in the study guide, try Exam4Labs's innovative testing engine for exam like NetSec-Analyst practice tests. These tests are made on the pattern of the Palo Alto Networks real exam and thus remain helpful not only for the purpose of revision but also to know the real exam scenario. To ensure excellent score in the exam, Exam4Labs's braindumps are the real feast for all exam candidates. They contain questions and answers on all the core points of your exam syllabus. Most of these questions are likely to appear in the NetSec-Analyst Real Exam.

>> NetSec-Analyst Study Tool <<

Here's The Proven And Quick Way To Get Success In Palo Alto Networks NetSec-Analyst Exam

Just like the old saying goes, motivation is what gets you started, and habit is what keeps you going. A good habit, especially a good study habit, will have an inestimable effect in help you gain the success. The NetSec-Analyst Study Materials from our company will offer the help for you to develop your good study habits. If you buy and use our study materials, you will cultivate a good habit in study.

Palo Alto Networks Network Security Analyst Sample Questions (Q115-Q120):

NEW QUESTION # 115
A critical, latency-sensitive application (App-ID: custom-app-1) must be deployed over a highly redundant SD-WAN architecture. The requirement is that this application must always use either MPLS Circuit A or MPLS Circuit B, based on which one has lower latency. If both MPLS circuits exceed a 50ms latency threshold OR if their combined packet loss exceeds 0.1%, traffic for this application must be automatically redirected to a dedicated, encrypted Internet VPN tunnel (Tunnel C) that serves as an emergency backup. If Tunnel C also fails its 100ms latency / 1% packet loss SLA, the traffic should be dropped. Which SD-WAN policy configuration best achieves this intricate failover and path preference logic?

- A. Create an SLA profile for custom-app-1 with thresholds: latency < 50ms (MPLS) and packet loss < 0.1% (MPLS), and latency < 100ms (Tunnel C) and packet loss < 1% (Tunnel C). Configure a PBF rule for custom-app-1 with primary next-hop as MPLS A, secondary as MPLS B, and tertiary as Tunnel C. PBF will handle the failover based on link health.
- B. Configure multiple security policies based on application and destination. Policy 1 for custom-app-1 will use a dedicated VR that only has MPLS A and B routes, with an SLA profile to detect degradation. Policy 2 for custom-app-1 will use a second VR that only has Tunnel C route, with its own SLA. Use route monitoring to switch between VRs based on SLA failure.
- C. Define two SD-WAN path groups: 'MPLS Preferred' containing MPLS A and B, and 'Internet_Backup' containing Tunnel C. Create an SD-WAN policy for custom-app-1. Set the primary path group to 'MPLS_Preferred' with a strict SLA (latency 50ms, loss 0.1%). Set the secondary path group to 'Internet_Backup' with a less strict SLA (latency 100ms, loss 1 Configure the 'Fail Action' to 'Drop' if all paths fail their respective SLAs. This allows the system to automatically failover based on group performance and then individual link performance.
- D. Use a PBF rule for custom-app-1. Set the primary egress interface to a zone containing MPLS A and B with a load-balancing algorithm based on latency. Configure a floating static route for custom-app-1 with a higher administrative distance pointing to Tunnel C, which becomes active if both MPLS interfaces go down. If Tunnel C fails, rely on default routing to drop the traffic.
- E. Configure a single SD-WAN policy for custom-app-1. Create a primary SLA profile for MPLS circuits (latency 50ms, loss 0.1%) and assign it to MPLS A and B. Create a secondary SLA profile for Tunnel C (latency 100ms, loss 1 and assign it to Tunnel Implement dynamic path selection where the 'best path' is chosen from MPLS NB first. If neither meets the primary SLA, the system automatically evaluates Tunnel C against its secondary SLA. If all fail, traffic drops.

Answer: C

Explanation:
Option B is the most appropriate and direct method using Palo Alto Networks SD-WAN features. By defining two distinct path groups with their respective SLA profiles, the system elegantly handles the complex failover logic. The primary path group 'MPLS_Preferred' with its strict SLA ensures that custom-app-1 always tries MPLS A or B first, based on performance. If both MPLS links within this group collectively (or individually, depending on the group's selection logic) fail to meet their combined SLA, the SD-WAN policy will automatically switch to evaluating the 'Internet_Backup' path group. Tunnel C then gets evaluated against its own, less stringent SLA. If Tunnel C also fails its SLA, the 'Fail Action' of 'Drop' ensures no traffic goes over an inadequate path. This leverages the hierarchical nature of SD-WAN path groups and their associated SLAs for robust, automated path selection and failover.

NEW QUESTION # 116
A network security architect is designing DoS protection for a critical API gateway behind a Palo Alto Networks firewall, which uses proprietary protocols over UDP on port 12345. The design requires a solution that: 1. Can identify and mitigate UDP floods targeting port 12345 based on packet rate. 2. Must differentiate between legitimate high-volume API calls from whitelisted partners and malicious floods. 3. Should NOT drop legitimate traffic, even under high load from partners. 4. Must automatically block sources identified as malicious for a configurable duration. Which combination of DoS protection profile elements and policy configuration in Palo Alto Networks firewall would best achieve these complex requirements?

- A. Configure a 'DoS Protection Policy' with a 'target' rule for the API gateway, enabling 'UDP Flood' protection (on port 12345) with 'group-by: source-ip'. Set 'Action: Block' with a 'Block Duration'. Additionally, create a higher-priority 'DoS Protection Policy' 'allow' rule for whitelisted partner IPs, with no DoS thresholds configured.
- B. Utilize a 'DoS Protection Profile' with 'UDP Flood' enabled and 'Action: Syn-Cookie' (for UDP). Apply this profile to a 'Security Policy' rule. Use a 'PBF' rule to direct whitelisted partner traffic around the DoS inspection.
- C. A 'Zone Protection' profile on the DMZ zone with 'UDP Flood' enabled, setting a high 'Per-Packet Rate' threshold. Implement 'DoS Protection Policy' 'whitelist' rules for known partner IP ranges, setting 'Action: Allow' for their traffic.
- D. Create a 'DoS Protection Policy' with a 'target' rule for the API gateway. Inside this rule, configure 'packet-based-attack-protection' for 'UDP Flood' (port 12345) with a 'Per-Packet Rate' and 'Action: Block' with a 'Block Duration'. Concurrently, define a 'DoS Protection Policy' 'exception' rule placed before the 'target' rule, specifying 'Source: Whitelisted_Partners_Address_Group' and 'Action: Allow'.

- E. A 'DoS Protection Policy' with a 'target' rule for the API gateway, enabling 'UDP Flood' protection with 'Per-Packet Rate' and 'Action: Drop'. Create a separate 'Security Policy' rule allowing whitelisted partners with 'No DoS Protection' applied.

Answer: D

Explanation:
This scenario demands granular control: specific UDP port, dynamic blocking, and whitelisting. 1. UDP Flood on specific port: Achieved by enabling 'UDP Flood' protection within 'packet-based-attack-protection' in a DoS Protection Policy, and potentially using a service object or specifying the port in the policy rule's service match. 2. Differentiate/Whitelist: This is the key. Palo Alto Networks DoS Protection Policies support 'allow' and 'exception' rules that are evaluated before 'target' rules. An 'exception' rule (or 'allow' rule depending on exact version/semantics) for whitelisted partners will bypass the DoS enforcement for their traffic. This rule must be placed with higher precedence. 3. Automatic Blocking: The 'Action: Block' with 'Block Duration' directly addresses this. Option E correctly combines these elements: a 'target' rule for the API gateway with specific UDP flood protection and automatic blocking, and a higher-priority 'exception' rule for whitelisted partners to ensure their legitimate high-volume traffic is allowed without DoS enforcement. Option A would still apply DoS to whitelisted traffic in the security rule. Option B uses Zone Protection, which is less granular, and 'whitelist' rules in DoS Policy are typically for bypassing DoS, not for general 'allow'. Option C's 'allow' rule approach is similar to E but 'exception' explicitly indicates bypassing, and 'no DoS thresholds configured' is crucial. Option D's 'Syn-Cookie' is TCP-specific and PBF is for traffic steering, not DoS bypass.

NEW QUESTION # 117
A financial institution has a requirement to send all traffic originating from the 'Finance' security zone, destined for external banking APIs (known IP ranges), through a dedicated, high-throughput internet link. Simultaneously, all other internet traffic from the 'Finance' zone should use the standard, lower-cost internet uplink. A PBF rule is configured as follows:

```
PBF Rule Name: Finance_API_Route
Source Zone: Finance
Destination Zone: Untrust
Source Address: any
Destination Address: 192.0.2.0/24, 203.0.113.0/24 (API IP ranges
Application: any
Service: any
Egress Interface: ethernet1/2 (High-throughput link)
Next Hop: 10.0.0.1
Action: Forward

PBF Rule Name: Finance_Default_Route
Source Zone: Finance
Destination Zone: Untrust
Source Address: any
Destination Address: any
Application: any
Service: any
Egress Interface: ethernet1/1 (Standard link)
Next Hop: 10.0.0.2
Action: Forward
```


After deployment, users in the 'Finance' zone report that some API traffic is still going over the standard link. What is the most probable cause for this misbehavior?

- A. The PBF rules are processed after security policy rules, causing the default security policy to take precedence for API traffic.
- B. The 'Finance_Default_Route' rule is placed above the 'Finance_API_Route' rule in the PBF policy rulebase.
- C. The 'Application' and 'Service' fields in the 'Finance_API_Route' rule should be more specific (e.g., 'web-browsing', 'ssl') to match API traffic accurately.
- D. PBF rules only apply to inter-zone traffic; intra-zone traffic destined for external IPs will bypass PBF.
- E. The 'Destination Zone' in both PBF rules should be explicitly set to 'any' instead of 'Untrust' for external destinations.

Answer: B

Explanation:

PBF rules, like security policy rules, are processed in order from top to bottom. If the 'Finance_Default_Route' (which has a broader 'Destination Address: any') is placed above 'Finance_API_Route' (which has specific API IP ranges), all traffic from the 'Finance' zone destined for 'Untrust' will match the 'Finance_Default_Route' first and be forwarded out the standard link, before the more specific API rule is ever evaluated. To fix this, 'Finance_API_Route' must be placed above 'Finance_Default_Route'. Option A is incorrect; PBF rules are processed before security policy rules. Option C is incorrect; 'Untrust' is typically the correct zone for external destinations. Option D is plausible for better granularity but not the most probable cause of all API traffic misdirection, especially if the API traffic is using standard HTTP/HTTPS. Option E is incorrect; PBF applies to traffic that matches the rule criteria, regardless of intra-zone or inter-zone if the destination is external and matches the rule.

NEW QUESTION # 118
A security analyst is developing an automated threat hunting script using the Strata Logging Service API. The script aims to identify suspicious file downloads (executables, scripts) from unapproved or unknown websites. The desired output is a list of sessions including the user, source IP, destination URL, and the WildFire verdict. Assuming a Python script is used, which API endpoint(s) and minimum set of query parameters are necessary to achieve this efficiently, and what should be the primary filter criteria in the query?

- A. API Endpoint: /log/threat and /log/url. Parameters: Separate queries for each, then manual correlation for 'file_type' and 'wildfire_verdict' from threat logs, and 'url_category' from URL logs.
- B.


- C.


- D.


- E.


Answer: C

Explanation:
The most efficient way to achieve this using Strata Logging Service is to query the combined 'data-lake' endpoint (which is the modern way to query all logs). The query should target 'wildfire.logs' which contain specific information about file analysis, including and 'verdict'. Including 'url_category eq 'unknown'' directly in the query is crucial for identifying downloads from unapproved/unknown sites. While 'threat' logs might have some WildFire info, 'wildfire.logs' are dedicated to this purpose and provide more detailed file analysis fields directly.

NEW QUESTION # 119
An advanced persistent threat (APT) group is suspected of exfiltrating data from an internal network segment to an external command- and-control (02) server over encrypted channels. The C2 communication leverages custom ports and rarely seen, but valid, SSL/TLS certificates. The security analyst has implemented SSL Forward Proxy decryption. Which specific configuration elements on the Palo Alto Networks firewall, beyond basic decryption policy, are critical to detect and prevent this sophisticated exfiltration attempt, potentially even if standard App-ID doesn't immediately identify it?

- A. All of the above combined, focusing on the synergy of decryption, content inspection, and threat intelligence. Specifically, full decryption allows App-ID to identify the true application, enabling granular policy enforcement and allowing Content-ID, Threat Prevention, File Blocking, and Data Filtering to inspect the domain/IP level. Custom signatures or advanced threat intelligence subscriptions are vital for detecting evasive C2.
- B. Enable 'Block Sessions with Unknown Status' in the decryption profile and ensure URL Filtering is configured to block 'Suspicious' categories.
- C. Configure a 'Security Policy' with 'Any' application and 'Decrypt' action, apply a custom 'Anti-Spyware' profile with DNS sinkholing, and enable 'Vulnerability Protection' with signatures for known C2 channels.
- D. Leverage 'File Blocking' profiles to prevent specific file types, enable 'Data Filtering' profiles for sensitive data patterns, and ensure 'Threat Prevention' is applied to the decrypted traffic. Additionally, consider custom 'External Dynamic Lists' for known C2 indicators.
- E. Ensure SSL Forward Proxy decryption is fully functional for the relevant zones. Utilize WildFire' analysis for unknown files, employ 'URL Filtering' to block suspicious or new domains, and apply a 'Custom URL Category' or 'External Dynamic List' for specific C2 domains/IPs. Configure 'Custom Signatures' based on threat intelligence for C2 patterns if available. Enable

'SSH Proxy' decryption for SSH tunnels.

Answer: A

Explanation:
This is a comprehensive scenario requiring a layered approach. Option E encompasses the most effective combination of features on a Palo Alto Networks firewall to combat sophisticated exfiltration over encrypted channels. Full decryption (SSL Forward Proxy) is the foundational element, as it enables all subsequent content inspection technologies (App-ID, Content-ID, Threat Prevention, File Blocking, Data Filtering) to see inside the encrypted tunnel. Without decryption, these features are severely limited. WildFire is critical for detecting zero-day malware used in exfiltration. URL Filtering and EDLs provide domain/IP reputation and blocking. Custom signatures are essential for detecting highly specific C2 patterns that might not be covered by standard databases. DNS sinkholing (from Anti-Spyware) is good, but without decryption, it might miss DNS over HTTPS. The synergy of all these features working on decrypted traffic provides the strongest defense against APTs.

NEW QUESTION # 120
.....

If you want to get NetSec-Analyst certification and get hired immediately, you've come to the right place. Exam4Labs offers you the best exam dump for NetSec-Analyst certification. With the guidance of no less than seasoned NetSec-Analyst professionals, we have formulated updated actual questions for NetSec-Analyst Certified exams, over the years. To keep our questions up to date, we constantly review and revise them to be at par with the latest NetSec-Analyst syllabus for NetSec-Analyst certification.

NetSec-Analyst New Braindumps Free: https://www.exam4labs.com/NetSec-Analyst-practice-torrent.html

Free demos and up to 1 year of free updates of our Sitecore Exams are also available at Exam4Labs NetSec-Analyst New Braindumps Free, And in fact, our NetSec-Analyst practice braindumps are quite interesting and enjoyable for our professionals have compiled them carefully with the latest information and also designed them to different versions to your needs, Once you submit your practice, the system of our NetSec-Analyst exam quiz will automatically generate a report.

thumb_up.jpg Good Practice Feeling confident about your financing NetSec-Analyst Relevant Questions because you work with a loan officer who is your advocate, who explains everything clearly, and who treats you right.

Plug-ins Scratch Disk, Free demos and up to 1 year of free updates of our Sitecore Exams are also available at Exam4Labs, And in fact, our NetSec-Analyst Practice Braindumps are quite interesting and enjoyable for our professionals have NetSec-Analyst Study Tool compiled them carefully with the latest information and also designed them to different versions to your needs.

Exam4Labs Palo Alto Networks NetSec-Analyst Exam Questions are Valid and Verified By Subject Matters Experts

Once you submit your practice, the system of our NetSec-Analyst exam quiz will automatically generate a report, We have to understand that not everyone is good at self-learning and self-discipline, and thus many people need NetSec-Analyst outside help to cultivate good study habits, especially those who have trouble in following a timetable.

Before you buy Exam4Labs Palo Alto Networks Certification Exam Study Guide, Dumps or the Practice Tests, you can download the free Palo Alto Networks NetSec-Analyst exam questions demo PDF file and examine the various features of our products.

- NetSec-Analyst Free Practice Exams □ NetSec-Analyst Free Practice Exams □ Free NetSec-Analyst Practice Exams □ Simply search for ➡ NetSec-Analyst □□□ for free download on ▸ www.examcollectionpass.com ◂ □NetSec-Analyst Valid Exam Labs
- Free NetSec-Analyst Practice Exams □ Technical NetSec-Analyst Training ☢ NetSec-Analyst Exam Book □ Immediately open ☀ www.pdfvce.com □☀□ and search for ➠ NetSec-Analyst □ to obtain a free download □ □NetSec-Analyst Exam Book
- Reliable NetSec-Analyst Test Sample □ New NetSec-Analyst Exam Camp □ Free NetSec-Analyst Practice Exams □ □ Easily obtain free download of ➡ NetSec-Analyst □□□ by searching on ☀ www.testkingpdf.com □☀□ □ □Preparation NetSec-Analyst Store
- Quiz Palo Alto Networks - NetSec-Analyst - Palo Alto Networks Network Security Analyst Pass-Sure Study Tool □ Copy URL ☀ www.pdfvce.com □☀□ open and search for 《 NetSec-Analyst 》 to download for free □NetSec-Analyst Exam Quick Prep
- NetSec-Analyst Study Tool - Quiz 2025 First-grade NetSec-Analyst: Palo Alto Networks Network Security Analyst New Braindumps Free □ Open ☀ www.itcerttest.com □☀□ enter ➥ NetSec-Analyst □ and obtain a free download □

□NetSec-Analyst Exam Quick Prep

- Valid NetSec-Analyst Test Labs □ NetSec-Analyst Latest Exam Tips □ Reliable NetSec-Analyst Test Sample □ Search for ▸ NetSec-Analyst ◂ and download exam materials for free through 「 www.pdfvce.com 」 □NetSec-Analyst Exam Quick Prep
- Valid NetSec-Analyst Exam Pass4sure ↙ NetSec-Analyst Valid Dumps Book □ Reliable NetSec-Analyst Test Sample □ □ Search for ➤ NetSec-Analyst □ and obtain a free download on □ www.testsimulate.com □ □NetSec-Analyst Latest Test Discount
- Valid NetSec-Analyst Test Labs □ NetSec-Analyst Latest Test Discount □ NetSec-Analyst Valid Exam Labs □ Open ➤ www.pdfvce.com □ and search for □ NetSec-Analyst □ to download exam materials for free □Exam NetSec-Analyst Fees
- NetSec-Analyst Study Tool - Quiz 2025 First-grade NetSec-Analyst: Palo Alto Networks Network Security Analyst New Braindumps Free □ Search on 「 www.pass4leader.com 」 for 「 NetSec-Analyst 」 to obtain exam materials for free download □NetSec-Analyst Latest Exam Tips
- NetSec-Analyst exam objective dumps - NetSec-Analyst valid pdf vce - NetSec-Analyst latest study torrent □ Search for ➥ NetSec-Analyst □ on ➠ www.pdfvce.com □ immediately to obtain a free download □Free NetSec-Analyst Updates
- Technical NetSec-Analyst Training □ Free NetSec-Analyst Practice Exams □ NetSec-Analyst Exam Quick Prep □ Easily obtain ➡ NetSec-Analyst □□□ for free download through ➥ www.torrentvce.com □ □Valid NetSec-Analyst Test Labs
- 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, 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, adamree449.blogofoto.com, penstribeacademy.com, learning.bivanmedia.com, szs.nxvtc.top, www.stes.tyc.edu.tw, shortcourses.russellcollege.edu.au, tedcole945.iyublog.com, www.stes.tyc.edu.tw, Disposable vapes