Authoritative NetSec-Analyst Valid Exam Sample, NetSec-Analyst Exam Dumps Collection

DOWNLOAD the newest RealExamFree NetSec-Analyst PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=17KDK8482B8v_zJhBdjDIIf-1YebmD3N4

Our Palo Alto Networks Network Security Analyst exam tool can support almost any electronic device, from iPod, telephone, to computer and so on. You can use Our NetSec-Analyst test torrent by your telephone when you are travelling far from home; I think it will be very convenient for you. You can also choose to use our NetSec-Analyst study materials by your computer when you are at home. You just need to download the online version of our NetSec-Analyst study materials, which is not limited to any electronic device and support all electronic equipment in anywhere and anytime. At the same time, the online version of our Palo Alto Networks Network Security Analyst exam tool will offer you the services for working in an offline states, I believe it will help you solve the problem of no internet. If you would like to try our NetSec-Analyst Test Torrent, I can promise that you will improve yourself and make progress beyond your imagination.

Palo Alto Networks NetSec-Analyst Exam Syllabus Topics:

Topic	Details
Topic 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.

Topic 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.
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	• 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.

NetSec-Analyst Exam Dumps Collection | NetSec-Analyst Reliable Braindumps Book

The latest NetSec-Analyst dumps collection covers everything you need to overcome the difficulty of real questions and certification exam. Accurate NetSec-Analyst test answers are tested and verified by our professional experts with the high technical knowledge and rich experience. You may get answers from other vendors, but our NetSec-Analyst briandumps pdf are the most reliable training materials for your exam preparation.

Palo Alto Networks Network Security Analyst Sample Questions (Q22-Q27):

NEW QUESTION # 22
What must be considered with regards to content updates deployed from Panorama?

- A. Panorama can only install up to five content versions of the same type for potential rollback scenarios.
- B. A PAN-OS upgrade resets all scheduler configurations for content updates.
- C. Content update schedulers need to be configured separately per device group.
- D. Panorama can only download one content update at a time for content updates of the same type.

Answer: D

NEW QUESTION # 23
An organization uses Palo Alto Networks firewalls and needs to enforce a strict data exfiltration prevention policy. They want to block any outgoing traffic that contains specific patterns of sensitive internal project codes, credit card numbers (PCI DSS scope), and social security numbers (PII scope). They have identified the following requirements: 1. Project codes (e.g., 'PROJ-ALPHA-2024-001', 'PROJ-BETA-FY25-ABC') follow a regex pattern: 2. Credit card numbers (16 digits) must be detected but only if they are associated with the 'PCI DATA ZONE' source zone. 3. Social security numbers (XXX-XX-XXXX) must be detected regardless of the source zone. Which combination of Data Filtering objects, profiles, and security policy rules would achieve this goal with the highest precision and minimal false positives, considering the specific zone requirement for credit cards?

- A. Create three Data Patterns: 'ProjectCode_Pattern' (Regex), 'CreditCard_Pattern' (Regex, pre-defined), 'SSN_Pattern' (Regex, pre-defined). Create two Data Filtering Profiles: 'Internal_Exfil Profile' with 'ProjectCode_Pattern' and 'SSN Pattern' enabled, and 'PCI Exfil Profile' with 'CreditCard_Pattern' enabled. Create two Security Policy rules: Rule 1: Source=Any,

Destination-Any, Action-Allow, Data Filtering Rule 2: Destination=Any, Action=Allow, Data Filtering Profile=PCI Exfil_Profile.

- B. Create three Data Patterns: 'ProjectCode_Pattern' (Regex: 'CreditCard_Pattern' (Pre-defined Data Pattern for Credit Card Numbers), 'SSN_Pattern' (Pre-defined Data Pattern for SSN). Create one Data Filtering Profile: 'Exfil_Prevention_Profile' with all three data patterns enabled and set to 'Block' action. Create two Security Policy rules: Rule 1: Name='PCI_Exfil_Block', Source=PCI_DATA_ZONE, Destination=Any, Service=Any, Application=Any, Action=Deny, Profile-Group (or specific profiles)=, Data Filtering Profile='Exfil_Prevention_Profile'. Rule 2: Name='General_Exfil_Block', Source=Any, Destination=Any, Service=Any, Application=Any, Action=Deny, Profile-Group (or specific profiles)=, Data Filtering Profile='Exfil_Prevention_Profile' (but for 'CreditCard_Pattern', set 'action' to 'alert' instead of 'block' within the rule's profile override for all sources EXCEPT 'PCI_DATA_ZONE').
- C. Create three Data Patterns: 'ProjectCode_Pattern' (Regex), 'CreditCard_Pattern' (Pre-defined), 'SSN Pattern' (Pre-defined). Create two Data Filtering Profiles: with 'ProjectCode_Pattern', 'CreditCard_Pattern', and 'SSN_Pattern' enabled. with 'ProjectCode_Pattern' and 'SSN Pattern' enabled. Create two Security Policy rules: Rule 1: Source=PCI DATA ZONE, Destination=Any, Action=Deny, Data Filtering Rule 2: Source-Any (excluding Destination-Any, Action-Deny, Data Filtering
- D. Create three Data Patterns: 'ProjectCode_Pattern' (Regex), 'CreditCard_Pattern' (Regex, pre-defined), 'SSN_Pattern' (Regex, pre-defined). Create one Data Filtering Profile: 'Comprehensive_Exfil_Profile' with all three data patterns enabled. Create two Security Policy rules: Rule 1: Source=PCI DATA ZONE, Destination=Any, Action=Deny, Data Filtering Profile=Comprehensive_Exfil_Profile. Rule 2: Source=Any, Destination=Any, Action=Deny, Data Filtering Profile=Comprehensive_Exfil Profile (with 'CreditCard_Pattern' disabled in this specific profile's application if possible, which is not directly supported).
- E. Create a custom Application object for each data type. Create three Security Policy rules: Rule 1: Source=PCI DATA ZONE, Destination=Any, Application=CreditCard_App, Action=Deny. Rule 2: Source=Any, Destination=Any, Application=ProjectCode_App, Action=Deny. Rule 3: Source=Any, Destination=Any, Application=SSN_App, Action=Deny.

Answer: C

Explanation:
This scenario requires granular control over data patterns based on source zones, which is best achieved by applying different Data Filtering profiles to different security policies. Let's break down why Option D is the most precise and why others fall short: Option D (Correct): Data Patterns: Correctly defines the three necessary data patterns: 'ProjectCode_Pattern' (custom regex), 'CreditCard_Pattern' (pre- defined for accuracy), and 'SSN_Pattern' (pre-defined). Data Filtering Profiles: Creates two distinct profiles: Includes all three patterns, ensuring that when traffic from 'PCI_DATA ZONE' is processed, all sensitive data types (including credit cards) are blocked. Includes only 'ProjectCode_Pattern' and 'SSN_Pattern'. This profile will be applied to traffic from all other zones, correctly preventing project code and SSN exfiltration without blocking credit cards from non-PCI zones. Security Policy Rules: Rule 1 (for PCI_DATA_ZONE): Matches traffic from and applies with a 'Deny' action, enforcing all three data pattern blocks. Rule 2 (for other zones): Matches traffic from 'Any' source (implicitly excluding what Rule 1 already matched due to rule order) and applies with a 'Deny' action, enforcing project code and SSN blocks only. This correctly separates the enforcement based on the source zone requirement. Why other options are incorrect: A: Using 'Allow' action with Data Filtering Profiles will only log or alert, not block, failing the 'prevent' requirement. Also, the profiles are designed to apply generally, not to deny based on pattern matches within an allow rule. B: While creating one comprehensive profile is possible, selectively disabling patterns within a profile's application per security rule for specific patterns (like disabling credit card detection for non-PCI zones) is not a standard, direct feature. You usually apply a profile as-is or override the action for the entire profile, not individual patterns within it. This approach would likely lead to over-blocking or misconfiguration. C: Similar to B, while the concept of overriding actions within a profile group per rule exists, precisely disabling a single pattern's action within a profile specifically for certain rules while keeping others active is overly complex and prone to error or not directly supported at that granularity. The cleaner approach is using separate profiles. E: Custom Application objects are for identifying applications (e.g., specific web services, proprietary protocols) based on signatures, not for detecting data patterns within application payload. Data filtering is the correct mechanism for this.

NEW QUESTION # 24
A Palo Alto Networks Network Security Analyst notices a pattern of 'DNS sinkhole' logs in the Log Viewer. These logs indicate internal hosts attempting to resolve known malicious domains, and the firewall is successfully redirecting these requests to the configured sinkhole IP. However, no corresponding 'critical' or 'high' severity alerts are appearing on the Incidents and Alerts page, despite the potential severity of internal compromise. What configuration element is MOST likely missing or misconfigured that would prevent these sinkhole events from generating an incident?

- A. The WildFire Analysis profile is not enabled for DNS traffic, so no verdict is generated.
- B. The DNS Proxy setting on the firewall is not enabled, preventing proper sinkholing.

- C. The Anti-Spyware profile applied to the relevant security policy does not have the 'DNS Sinkhole' action set to 'alert' or 'block' for the respective threat category.
- D. The Security Policy rule allowing DNS traffic has its 'Action' set to 'allow' instead of 'allow-log'.
- E. The Log Fomarding profile is not configured to send 'threat' logs with 'severity: high' to the Cortex Data Lake for incident correlation.

Answer: C

Explanation:
DNS Sinkholing is a feature of the Anti-Spyware profile. For DNS sinkhole events to generate alerts and incidents, the Anti-Spyware profile applied to the security policy allowing the DNS traffic must be configured to take an 'alert' or 'block' action when a DNS sinkhole event occurs. If the action is set to 'default' and the default does not include alerting, or if it's set to 'allow' without logging an alert, then no incident will be generated, even if the sinkholing itself is successful and logged. Option A is incorrect because sinkholing is occurring and logs are generated. Option C is plausible if no threat logs were generated at all, but here logs exist, just not alerts. Option D is irrelevant to basic DNS sinkhole alerting. Option E affects logging, but not the generation of an alert from a security profile's action.

NEW QUESTION # 25
A global corporation operates a distributed network with multiple Palo Alto Networks firewalls. A centralized logging server (syslog-server.example.com, 198.51.100.10) for all security devices is located in a datacenter, accessible via an MPLS VPN tunnel (tunnel.2) from all branch offices. Network administrators want to ensure that syslog traffic from the firewall itself (source 192.168.1.1 , management interface) to syslog-server.example.com always uses tunnel.2, bypassing the default route to the internet, even if the logging server resolves to a public 12 This must be resilient to tunnel outages. All other management traffic should use the default route. Which configuration elements are necessary and in what order of evaluation to ensure this PBF works correctly?

- A. 1. Define a PBF rule in the 'Policies' tab matching Source Zone: Management, Source Address: 192.168.1.1 , Destination FQDN: syslog-server.example.com, Application: syslog, Egress Interface: tunnel.2, Next Hop: (MPLS Router IP in datacenter), Action: Forward, Fall back to: No. 2. Configure 'Device > Setup > Management > Services > Logging' to use syslog-server.example.com.
- B. 1. Define a PBF rule in the 'Policies' tab matching Source Address: 192.168.1.1, Destination FQDN: syslog-server.example.com, Application: syslog, Egress Interface: tunnel.2, Next Hop: (MPLS Router IP in datacenter), Action: Forward, Fall back to: Discard. 2. Ensure a Security Policy rule allows this traffic.
- C. 1. Define a PBF rule in the 'Policies' tab matching Source Address: 192.168.1.1 , Destination FQDN: syslog-server.example.com, Application: syslog, Egress Interface: tunnel.2, Next Hop: (MPLS Router IP in datacenter), Action: Forward, Fall back to: Default (Virtual Router). 2. Configure the firewall's logging profile to send to syslog-server.example.com. 3. Critically, set the 'Service Route' for 'Syslog' under 'Device > Setup > Management' to 'Management Interface' to ensure PBF evaluation for firewall-generated traffic.
- D. 1. Configure a PBF rule in the 'Policies' tab matching Source Address: 192.168.1.1, Destination Address: 198.51.100.10, Application: syslog, Egress Interface: tunnel.2, Next Hop: (MPLS Router IP in datacenter), Action: Forward, Fall back to: 'Next VR' with the default virtual router. 2. Define a Static Route for 198.51.100.10 via tunnel.2 with a higher metric.
- E. 1. Configure a 'Service Route' under 'Device > Setup > Management' for syslog-server.example.com via the 'tunnel.2' interface. 2. Create a PBF rule to match the syslog traffic, applying it to the appropriate zone.

Answer: C

Explanation:
This is a very tricky question because it involves firewall-generated traffic (management plane). 1. PBF for Firewall-Generated Traffic: For firewall-generated traffic (like syslog, SNMP, DNS queries, updates), PBF rules are only evaluated if the 'Service Route' for that specific service is set to 'Management Interface' or 'Data Plane Interface'. If it's set to 'Source IP' or 'Default', PBF rules for that traffic are bypassed, and standard routing table lookup (based on the source interface's VR) occurs. Therefore, setting the 'Service Route' for Syslog to 'Management Interface' (or the relevant data plane interface if syslog comes from a dataplane IP) is crucial. 2. PBF Rule Definition: The PBF rule itself (Option E's PBF description) is well-formed: it matches the source IP of the firewall's management interface, the FQDN of the syslog server, the 'syslog' application, and specifies the egress tunnel and next-hop. 'Fall back to: Default (Virtual Router)' would mean if the tunnel fails, it goes via the standard route, which is generally acceptable for syslog if blocking isn't explicitly required. 3. Order of Evaluation: The service route decision happens first for firewall-generated traffic. If it points to an interface that belongs to a virtual router, then PBF rules for that virtual router are consulted, followed by the VR's routing table. Option A and C are incorrect because they miss the critical 'Service Route' configuration for firewall-generated traffic. Option B incorrectly implies a 'Service Route' alone can achieve the specific routing (it can, but not with PBF granularity/fallback) or that PBF would apply without it being explicitly set to 'Management Interface'. Option D suggests a static route, which wouldn't be as flexible as PBF for application-specific FQDN-based routing and wouldn't provide the explicit

PBF fallback control.

NEW QUESTION # 26
An administrator would like to see the traffic that matches the interzone-default rule in the traffic logs.
What is the correct process to enable this logging1?

- A. Select the interzone-default rule and edit the rule on the Actions tab select Log at Session End and click OK
- B. This rule has traffic logging enabled by default no further action is required
- C. Select the interzone-default rule and edit the rule on the Actions tab select Log at Session Start and click OK
- D. Select the interzone-default rule and click Override on the Actions tab select Log at Session End and click OK

Answer: D

NEW QUESTION # 27
.....

Our NetSec-Analyst learning quiz is the accumulation of professional knowledge worthy practicing and remembering, so you will not regret choosing our NetSec-Analyst study guide. The best way to gain success is not cramming, but to master the discipline and regular exam points of question behind the tens of millions of questions. Our NetSec-Analyst Preparation materials can remove all your doubts about the exam. If you believe in our products this time, you will enjoy the happiness of success all your life