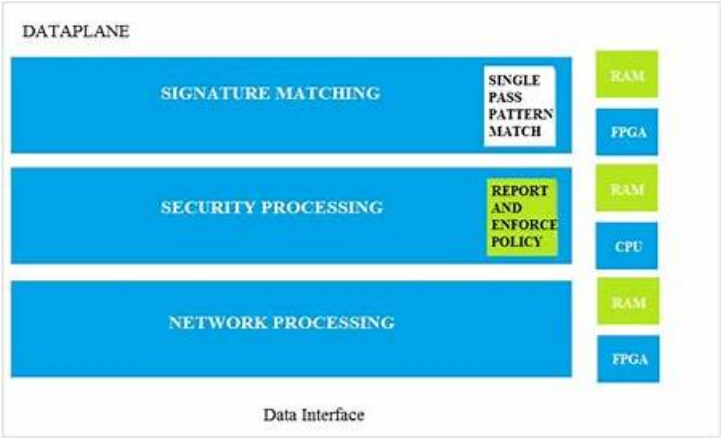
NetSec-Analyst Reliable Braindumps Ebook, NetSec-Analyst Actual Braindumps



BTW, DOWNLOAD part of Test4Cram NetSec-Analyst dumps from Cloud Storage: https://drive.google.com/open?id=1TcFl7Idt0zXrB51BShn7KG6m_GB5nYIB

Life of future will definitely be much more easy and convenient than the life of today, it is not late whenever you want to work as an IT engine. Our NetSec-Analyst exam questions and answers help you realize your dream easily. We Test4Cram offer the top-class exam materials similar with the real test. NetSec-Analyst Exam Questions And Answers assist people to master the real test questions and key knowledge so that candidates will fell easy and casual in real test so that they can clear exams and obtain a Palo Alto Networks certification certainly.

Palo Alto Networks NetSec-Analyst Exam Syllabus Topics:

Section	Objectives
Centralized Management	- Configuration Management - Panorama Management - Device Groups and Templates - Strata Cloud Manager (SCM)
Policy Creation and Application	- Security Policies - Decryption Policies - QoS Policies - NAT Policies
Operations and Troubleshooting	- Security Policy Troubleshooting - Traffic Analysis - Log Analysis - Connectivity Issues
Strata Logging Service	- Log Forwarding - Log Analysis and Reporting - Integration with SCM
Security Posture Improvement	- Data Filtering - WildFire Analysis - Threat Prevention - URL Filtering
Object Configuration	- Custom Objects - Address Objects - Application Objects - Service Objects

>> NetSec-Analyst Reliable Braindumps Ebook <<

NetSec-Analyst Actual Braindumps - NetSec-Analyst Latest Exam Book

In order to let you have a deep understanding of our NetSec-Analyst learning guide, our company designed the free demos for our customers. We will provide you with free demos of our study materials before you buy our products. If you want to know our NetSec-Analyst training materials, you can download them from the web page of our company. If you use the free demos of our NetSec-Analyst study engine, you will find that our products are very useful for you to pass your NetSec-Analyst exam and get the certification.

Palo Alto Networks Network Security Analyst Sample Questions (Q26-Q31):

NEW QUESTION # 26
A sophisticated zero-day attack is suspected to be propagating laterally within your network. You need to quickly identify all active network connections, their associated applications, users, and any related threats, across your distributed environment. Then, you need to rapidly quarantine affected hosts and block the identified malicious application signature. Which set of tools and features provides the most efficient and comprehensive response?

- A. 1. Review firewall logs for 'deny' entries. 2. Use Wireshark on affected hosts for packet capture. 3. Manually update security policies on each firewall.
- B. 1. Command Center: 'Threat Activity' and 'Network Activity' dashboards for real-time anomalous traffic. 2. Use dynamic filters in Command Center to pinpoint source/destination IPs, users, and applications. 3. Implement External Dynamic Lists (EDLs) or a custom Anti-Spyware profile for rapid IP/URL blocking. 4. Create Security Policy rules to quarantine infected hosts (e.g., move to a quarantine zone or block all traffic).
- C. 1. Activity Insights: Generate 'User Activity' reports for suspicious logins. 2. Policy Optimizer: Recommend rules to block specific user activity. 3. Manually block user accounts.
- D. 1. Command Center: 'Network Activity' dashboard filtered for high session count. 2. Activity Insights: Review 'Top Applications' for anomalies. 3. Policy Optimizer: Create a new 'Deny' rule for the suspicious application.
- E. 1. Command Center: Focus on 'Application Usage' dashboard to detect new applications. 2. Manually configure a URL filtering profile to block suspicious websites. 3. Isolate the network segment.

Answer: B

Explanation:
This scenario requires a rapid, comprehensive incident response. Command Center is paramount for real-time visibility into 'Threat Activity' and 'Network Activity' to quickly identify ongoing propagation, including applications and users. Its dynamic filtering capabilities are essential for pinpointing affected entities. For rapid blocking of indicators of compromise (IPs, URLs), EDLs or custom Anti-Spyware profiles are highly effective. Finally, creating Security Policy rules to quarantine or block traffic to/from infected hosts is the direct action needed to contain the lateral movement. Activity Insights is more for trend analysis, and Policy Optimizer is for policy refinement, not immediate incident response to a zero-day.

NEW QUESTION # 27
An administrator would like to use App-ID's deny action for an application and would like that action updated with dynamic updates as new content becomes available.
Which security policy action causes this?

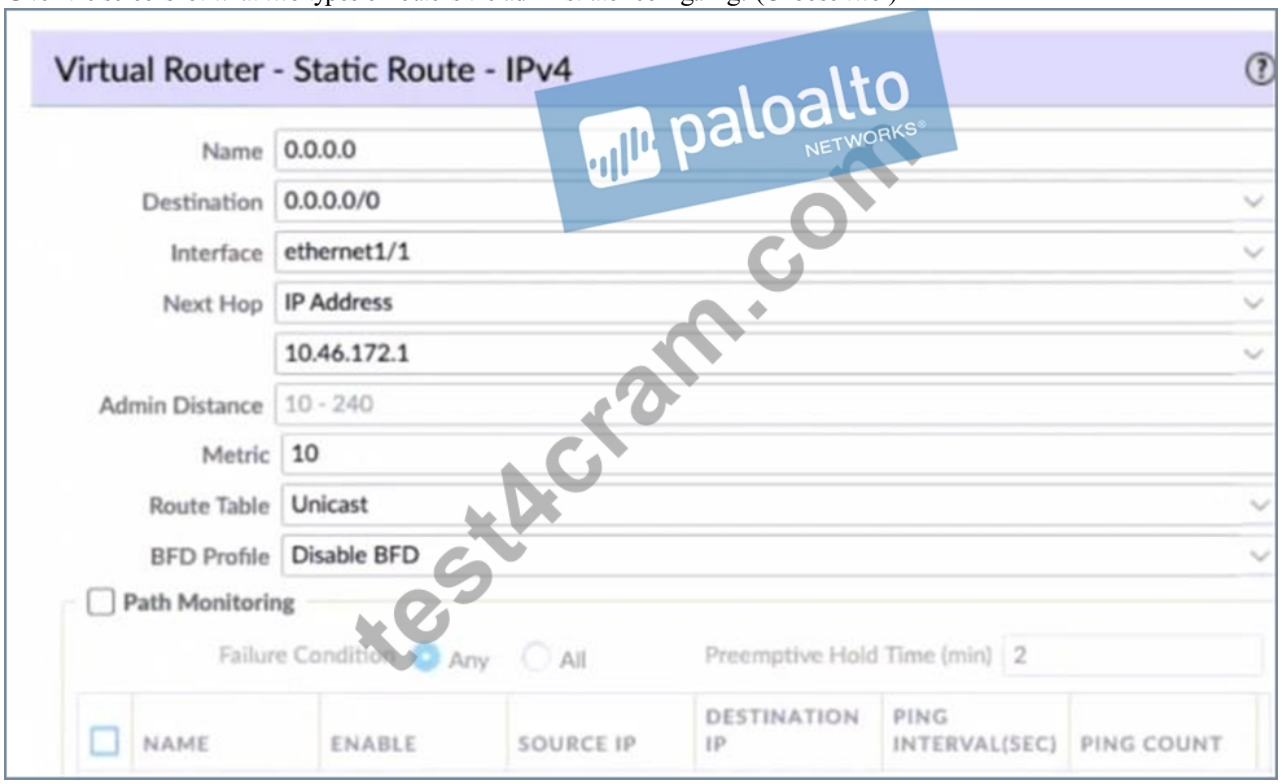
- A. Reset server
- B. Drop
- C. Deny
- D. Reset both

Answer: C

Explanation:
Explanation/Reference:
Reference:
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/manage- configuration backups/revert-firewall-configuration- changes.html

NEW QUESTION # 28

Given the screenshot what two types of route is the administrator configuring? (Choose two)



- A. static route
- B. default route
- C. BGP
- D. OSPF

Answer: B

NEW QUESTION # 29
A security analyst is configuring decryption policies on a Palo Alto Networks firewall to prevent the exfiltration of sensitive data through encrypted channels. They encounter a scenario where an internal application, using self-signed certificates, needs to communicate with an external cloud service over TLS. Decrypting this traffic with a traditional 'SSL Forward Proxy' profile causes application failures. Which decryption mode and associated configuration would be most appropriate to inspect this traffic without breaking the application, while still ensuring sensitive data protection?

- A. SSL No Decryption with the 'Forward Proxy' decryption profile and a custom 'Decryption Policy' rule to decrypt this specific traffic.
- B. SSL Forward Proxy with the 'SSL Protocol Settings' configured to 'Block Sessions with Untrusted Certificates'.
- C. SSL Decryption Exclusions based on URL Category for the cloud service.
- D. SSL Inbound Inspection with a custom certificate profile for the internal application's self-signed certificates.
- E. SSL Forward Proxy with the 'No Decryption' action for the specific application traffic.

Answer: D

Explanation:
For internal applications using self-signed certificates that need decryption, SSL Inbound Inspection is the correct approach. Instead of the firewall re-signing traffic with its own root CA (which would break trust for the self-signed certs), Inbound Inspection requires importing the internal application's private key and certificate onto the firewall. This allows the firewall to decrypt and inspect the traffic originating from that internal application without disrupting its trust chain with the external service. Options A, C, and D either disable inspection or are more suited for general outbound traffic. Option E is contradictory as 'No Decryption' would prevent inspection.

NEW QUESTION # 30

A Palo Alto Networks firewall administrator is troubleshooting an issue where a newly deployed containerized application's traffic (TCP/8443) is intermittently identified as 'ssl' and sometimes as 'unknown-tcp', even though the application always uses the same proprietary TLS certificate and handshake. This inconsistency leads to erratic policy enforcement and dropped connections. The administrator suspects a race condition or an App-ID engine limitation with highly dynamic container environments. Which of the following advanced Application Override configurations, if applicable, would be the most effective in ensuring consistent identification of this proprietary application as 'custom-app-tls' (a pre-defined custom application)?

- A. Implement a PBF (Policy Based Forwarding) rule to steer the container traffic to a specific security zone where App-ID is disabled for TCP/8443.
- B. An Application Override configured with 'Source IP', 'Destination IP', 'Service' (TCP/8443), and specifying the custom application 'custom-app-tls', but prioritizing it lower than default App-ID.
- C. A simple Application Override for TCP/8443 to 'custom-app-tls' for all traffic.
- D. A custom application signature created specifically to identify the proprietary TLS handshake and certificate chain of the containerized application, applied globally.
- E. An Application Override configured with the following CLI command structure:

```
set application-override rule 'container-app-override' application 'custom-app-tls' protocol tcp port 8443 source-zone 'container-zone'
destination-zone 'app-backend-zone' priority high
```

Answer: E

Explanation:
The key here is 'intermittently identified' and 'race condition/engine limitation', suggesting that a standard override might still compete with App-ID. Option C introduces the 'priority high' option (though in a slightly simplified CLI format for clarity, the concept of override rule order/precedence is critical) which ensures that this specific override rule takes precedence over App-ID's default classification process for the defined traffic. This is crucial for ensuring consistent identification in challenging scenarios. Option A is too broad and doesn't account for the intermittent issue. Option B with 'priority lower' would be ineffective. Option D is a valid alternative but is more complex to implement and maintain than an override, especially if the 'signature' relies on subtle, potentially changing aspects. Option E bypasses App-ID entirely, losing visibility and control.

NEW QUESTION # 31
.....

Open { www.pdfvce.com } and search for " NetSec-Analyst " to download exam materials for free □NetSec-Analyst Exam Training

- Test NetSec-Analyst Vce Free □ NetSec-Analyst Exam Study Solutions □ NetSec-Analyst Valid Braindumps Book □ □ Search for ⇛ NetSec-Analyst ⇚ and obtain a free download on 【 www.vce4dumps.com 】 □Exam NetSec-Analyst Blueprint
- Fantastic NetSec-Analyst Reliable Braindumps Ebook - Leader in Qualification Exams - Unparalleled NetSec-Analyst Actual Braindumps □ Immediately open □ www.pdfvce.com □ and search for ☀ NetSec-Analyst □☀□ to obtain a free download ☯ Valid NetSec-Analyst Exam Review
- Palo Alto Networks Realistic NetSec-Analyst Reliable Braindumps Ebook Free PDF Quiz □ Download ▸ NetSec-Analyst ◂ for free by simply entering ➽ www.exam4labs.com □ website □NetSec-Analyst Simulations Pdf
- 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, 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, Disposable vapes

BTW, DOWNLOAD part of Test4Cram NetSec-Analyst dumps from Cloud Storage: https://drive.google.com/open?id=1TcFl7Idt0zXrB51BShn7KG6m_GB5nYIB