Hot NetSec-Analyst Exam Questions Vce 100% Pass | Reliable NetSec-Analyst: Palo Alto Networks Network Security Analyst 100% Pass

It is our company that can provide you with special and individual service which includes our NetSec-Analyst preparation quiz and good after-sale services. Our experts will check whether there is an update every day, so you needn't worry about the accuracy of NetSec-Analyst Study Materials. If there is an update system, we will send them to the customer automatically. As is known to all, our NetSec-Analyst simulating materials are high pass-rate in this field, that's why we are so famous.

Palo Alto Networks NetSec-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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.

Training NetSec-Analyst Materials, Test NetSec-Analyst Pattern

As for Palo Alto Networks NetSec-Analyst exam, it is the most difficult to pass. But, as long as you believe in Dumpkiller, everything is ok. Dumpkiller Palo Alto Networks NetSec-Analyst exam simulations contain the most accurate questions and answers. If you don't believe our Palo Alto Networks NetSec-Analyst certification training, you can go to our Dumpkiller. You can find pdf real questions and answers and download it. And the purchase rate is unbelievably high every day. By choosing it, pass rate is 100%. Hurry up! Don't hesitate to add our Palo Alto Networks NetSec-Analyst Dumps Torrent to your shopping cart.

Palo Alto Networks Network Security Analyst Sample Questions (Q171-Q176):

NEW QUESTION # 171
A Palo Alto Networks firewall is configured with IPSec VPN tunnels to multiple branch offices. Users in a specific branch office are reporting intermittent connectivity issues to resources in the main data center. 'show vpn flow' on the main data center firewall shows the VPN tunnel state as 'Up', but the 'Rx Bytes' and 'Tx Bytes' are not incrementing for traffic from the affected branch. 'show log traffic direction equal reverse' on the main firewall also shows no matching traffic for the branch network's return path. What is the MOST complex and difficult-to-diagnose underlying network issue that could cause this scenario?

- A. A duplicate IP address conflict exists on the branch office network, causing routing instability.
- B. The 'security-zone' configuration on the tunnel interface on either end of the VPN has been changed or removed, breaking policy enforcement.
- C. The branch office firewall's local proxy ID or remote proxy ID configuration is incorrect for the main data center's subnets.
- D. An upstream ISP routing change or BGP flap on the branch office's internet connection is intermittently black-holing traffic destined for the main data center's public IP address.
- E. The pre-shared key (PSK) on one end of the VPN tunnel has been changed, leading to decryption failures.

Answer: D

Explanation:
The most difficult-to-diagnose issue among the choices, given the symptoms, is an intermittent upstream routing problem (D). If the VPN tunnel itself shows 'Up' and 'Rx/Tx Bytes' are not incrementing for traffic , it means traffic isn't reaching the tunnel or isn't successfully traversing it. Options A, C, and E would typically cause the VPN tunnel itself to go down or prevent any traffic. Option B is an internal issue for the branch, but wouldn't manifest as no Rx/Tx bytes on the main firewall's VPN tunnel interface unless it completely prevented all branch traffic from reaching the internet. Option D, an intermittent ISP routing change, could cause traffic to the main data center's public IP (the VPN peer) to be dropped before it even reaches the branch firewall, or return traffic from the main data center to the branch firewall to be lost. This would explain 'Up' tunnel but no traffic, and no matching reverse traffic logs, as the packets aren't successfully traversing the public internet path to initiate or maintain the encrypted flow within the tunnel. Diagnosing this often requires collaboration with ISPs and traceroutes from multiple points.

NEW QUESTION # 172
Which statement best describes a common use of Policy Optimizer?

- A. Policy Optimizer can add or change a Log Forwarding profile for each Security policy selected.
- B. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exists. Admins can then manually enable policies they want to keep and delete ones they want to remove.
- C. Policy Optimizer can display which Security policies have not been used in the last 90 days.
- D. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications.

Answer: C

NEW QUESTION # 173
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 DNS Proxy setting on the firewall is not enabled, preventing proper sinkholing.
- B. The WildFire Analysis profile is not enabled for DNS traffic, so no verdict is generated.
- C. The Security Policy rule allowing DNS traffic has its 'Action' set to 'allow' instead of 'allow-log'.
- D. 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.
- E. The Log Forwarding profile is not configured to send 'threat' logs with 'severity: high' to the Cortex Data Lake for incident correlation.

Answer: D

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 # 174
Which two addresses should be reserved to enable DNS sinkholing? (Choose two.)

- A. MAC
- B. Email
- C. IPv4
- D. IPv6

Answer: C,D

Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGECA0

NEW QUESTION # 175
Which object would an administrator create to block access to all high-risk applications?

- A. application group
- B. HIP profile
- C. application filter
- D. Vulnerability Protection profile

Answer: C

Explanation:
Explanation/Reference:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKECA0

NEW QUESTION # 176
......

There are a lot of excellent experts and professors in our company. In the past years, these experts and professors have tried their best to design the NetSec-Analyst exam questions for all customers. More importantly, we believe once you finally gain the NetSec-Analyst certification with our NetSec-Analyst exam questions and you will find enormous benefits: more enjoyment of life and better relationships and less stress and a better quality of life overall. So it is very significant for you to do everything in your power to pass the NetSec-Analyst Exam and get the related certification.

Training NetSec-Analyst Materials: https://www.dumpkiller.com/NetSec-Analyst_braindumps.html