Valid NetSec-Analyst Exam Tips | NetSec-Analyst Detailed Answers

Total No. of Questions : 8] SEAT No. :

PC1808 [6353]-127 [Total No. of Pages :2

T.E. (Information Technology)

COMPUTER NETWORKS AND SECURITY

(2019 Pattern) (Semester- II) (314451)

Time : 2½ Hours] *[Max. Marks : 70*

Instructions to the candidates:

1) *Answer Q.1 or 2, Q.3 or 4, Q.5 or 6, Q.7 or 8.*
2) *Neat diagrams must be drawn wherever necessary.*
3) *Figures to the right side indicate full marks.*
4) *Assume Suitable data if necessary.*

Q1) a) Explain DSDV (Destination Sequenced Distance Vector) with connection establishment and data transfer phase in detail. [9]

b) Comment on Adhoc Network MAC Layer with Design Issues, Design Goal. [9]

OR

Q2) a) Briefly explain classification of routing protocol for AdHoc Wireless Networks. [6]

b) Explain with diagram Clustered Architecture of Sensor Network. [6]

c) Write a short note on MACAW. [6]

Q3) a) What is stream Cipher? Explain the encryption process using stream Cipher with suitable example. [8]

b) What is Cipher Feedback Mode(CFM)? Explain the process of CFM with suitable example. [9]

OR

Q4) a) Write comparison between symmetric and asymmetric key cryptography. [5]

b) Define Network Attack. Explain with suitable example what do you mean by Active attacks and Passive attacks? [6]

c) Describe the following network security threats: [6]

i) Unauthorized access
ii) Distributed denial of service
iii) Man in the middle

P.T.O.

BONUS!!! Download part of CramPDF NetSec-Analyst dumps for free: https://drive.google.com/open?id=1BQQf4Dmc1ruFzL2XwNQvQfDUbrqt6JAl

As a top selling product in the market, our NetSec-Analyst study guide has many fans. They are keen to try our newest version products even if they have passed the NetSec-Analyst exam. They never give up learning new things. Every time they try our new version of the NetSec-Analyst Real Exam, they will write down their feelings and guidance. Also, they will exchange ideas with other customers. And in such a way, we can develop our NetSec-Analyst practice engine to the best according to their requirements.

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.

Providing You Authoritative Valid NetSec-Analyst Exam Tips with 100% Passing Guarantee

Our experts are not slavish followers who just cut and paste the content into our NetSec-Analyst practice materials, all NetSec-Analyst exam questions are elaborately compiled by them. Just a small amount of money, but you can harvest colossal success with potential bright future. So we have the courage and justification to declare the number one position in this area, and choosing NetSec-Analyst Actual Exam is choosing success.

Palo Alto Networks Network Security Analyst Sample Questions (Q39-Q44):

NEW QUESTION # 39
A Security Analyst observes a high volume of 'threat' logs in the Palo Alto Networks Log Viewer, specifically for 'vulnerability' type, originating from a single internal subnet (10.10.10.0/24) targeting external IPs. However, no corresponding 'critical' or 'high' severity alerts are visible on the Incidents and Alerts page. What is the MOST likely reason for this discrepancy and what initial steps should the analyst take?

- A. The Incidents and Alerts page automatically filters out 'vulnerability' threats unless they are part of a larger correlated attack. The analyst should manually create an incident from the log viewer.
- B. There is a network connectivity issue between the firewall and the management plane, preventing incident synchronization. The analyst should check network reachability and firewall health.
- C. The security policy governing the subnet (10.10.10.0/24) is configured in 'alert only' mode for this threat signature, preventing an incident from being generated. The analyst should review the policy configuration and consider changing the action to 'block' or 'reset-both'.
- D. The Log Fomarding profile is misconfigured and not sending threat logs to the Cortex Data Lake for incident correlation. The analyst should verify Log Forwarding settings.
- E. The threat logs are false positives, and no action is required beyond reviewing the log details.

Answer: C

Explanation:
The most likely reason for threat logs appearing without corresponding alerts on the Incidents and Alerts page is that the security policy's action for that specific threat signature or vulnerability type is set to 'alert only' instead of 'block', 'reset-client', or 'reset-

both'. This means the firewall detects the threat and logs it, but it doesn't take an enforcement action or generate an incident unless explicitly configured to do so. The initial step should be to investigate the relevant security policy and its associated profiles (e.g., Vulnerability Protection profile) to confirm the action taken when this threat signature is matched. Options C and A are less likely given the high volume. Option D is incorrect because logs are visible in the Log Viewer, implying successful forwarding to CDL. Option E is unlikely if logs are being actively received.

NEW QUESTION # 40
A critical industrial control system (ICS) network, isolated from the internet, requires extremely low latency and high availability. While internal DoS attacks are rare, a misconfigured or rogue device could potentially flood the network. The security team wants to implement a DoS protection profile that proactively identifies and drops unusually high rates of UDP traffic targeting specific ICS application ports, without introducing any significant processing overhead or latency. Which configuration approach in Palo Alto Networks firewall DoS protection would best achieve this goal?

- A. Utilize 'Packet Based Attack Protection' within a 'DoS Protection Policy' rule, targeting 'UDP Flood' on specific destination ports, and configure a 'Per-Packet Rate' threshold with 'Action: Drop'.
- B. Configure a 'Zone Protection' profile for the ICS zone with 'Flood Protection' enabled for 'UDP Flood', setting a 'Per-Packet Rate' threshold and 'Action: Drop'.
- C. Create a 'DoS Protection Policy' rule with 'Packet Based Attack Protection' for 'UDP Flood' and specify the target application ports, setting 'Action: Syn-Cookie' to mitigate.
- D. Apply an 'IP Address Block' profile to the ICS interface, monitoring for any source IP exceeding a 'Session Rate' of 100 sessions/second and blocking for 300 seconds.
- E. Implement a 'Data Filtering' profile to identify specific UDP payload patterns associated with ICS applications and block traffic not conforming to these patterns.

Answer: A

Explanation:
The requirement is to proactively identify and drop high rates of UDP traffic on specific application ports with low latency. 'Packet Based Attack Protection' within a 'DoS Protection Policy' is the most granular and efficient way to achieve this. By targeting 'UDP Flood' and specifying destination ports, the firewall can quickly identify and drop excessive UDP packets without the overhead of session tracking or SYN- cookie mechanisms (which are for TCP). Option A (Zone Protection) provides less granularity on specific ports. Option B incorrectly suggests 'Syn- Cookie' for UDP. Option C (IP Address Block) is reactive and might block legitimate devices due to misconfiguration. Option D (Data Filtering) is for content inspection, not volume-based DoS. Option E precisely matches the requirements for efficient, targeted UDP flood protection.

NEW QUESTION # 41
A company wants to ensure that any file uploaded to a specific cloud storage provider is immediately analyzed for malware, even if the file has never been seen before. Which action should be set in the WildFire Analysis Profile?

- A. Forward
- B. Continue
- C. Alert
- D. Block

Answer: A

Explanation:
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
In a WildFire Analysis Profile, the primary action for unknown files is to Forward them to the WildFire cloud for sandbox analysis. Unlike a standard "block" or "allow" action, forwarding initiates a behavioral analysis to determine if the file exhibits malicious characteristics.
For an analyst, the objective is to ensure that all relevant file types (PDFs, executables, etc.) are set to forward. If WildFire determines a file is malicious, it generates a new signature in as little as 5 minutes and pushes it to all firewalls globally. Some advanced implementations allow for "inline" blocking of files until the WildFire result is returned, but the fundamental configuration step for all zero-day protection is the forwarding of unknown content to the threat intelligence cloud.

NEW QUESTION # 42

A Palo Alto Networks firewall is suffering from high CPU utilization due to an excessive volume of logs being processed and forwarded. An investigation reveals that a Log Forwarding Profile is forwarding all log types, including debugging logs, to a remote syslog server. To optimize performance without completely disabling logging, which of the following is the most effective adjustment to the existing Log Forwarding Profile?

- A. Change the log forwarding protocol from UDP to TCP for reliability, as dropped UDP packets cause retransmissions and higher CPU.
- B. Reduce the number of Security Policies that utilize this Log Forwarding Profile.
- C. Implement a custom filter within the Log Forwarding Profile to exclude verbose log types like 'debug' or 'pkt-diag' using expressions such as
  `(log.type neq 'debug' and log.type neq 'pkt-diag')`
- D. Increase the log buffer size on the firewall to temporarily store more logs, reducing immediate forwarding load.
- E. Configure a Log Rate Limit on the firewall to cap the total logs per second being forwarded.

Answer: C

Explanation:
Option C directly addresses the root cause: excessive logging of unnecessary log types. By excluding verbose log types like 'debug' or 'pkt-diag' directly within the Log Forwarding Profile's filter, the firewall will stop processing and forwarding these specific logs, significantly reducing the log volume and associated CPU load. Option A (TCP vs UDP) affects reliability but not necessarily volume. Option B (buffer size) only defers the problem. Option D (reducing policies) would prevent necessary logging. Option E (Log Rate Limit) is a throttling mechanism that might drop logs if the rate is exceeded, which isn't ideal for compliance, and doesn't solve the issue of generating too many logs to begin with.

NEW QUESTION # 43
Which administrator type provides more granular options to determine what the administrator can view and modify when creating an administrator account?

- A. Role-based
- B. Root
- C. Dynamic
- D. Superuser

Answer: A

NEW QUESTION # 44
.....

for ➤ NetSec-Analyst □ and obtain a free download on ➡ www.pdfvce.com □□□ □NetSec-Analyst Exam Questions

- First-grade Valid NetSec-Analyst Exam Tips by www.troytecdumps.com □ The page for free download of ➽ NetSec-Analyst □ on （ www.troytecdumps.com ） will open immediately □NetSec-Analyst Dump File
- Valid NetSec-Analyst Exam Tips - First-grade Palo Alto Networks NetSec-Analyst Detailed Answers Pass Guaranteed □ Simply search for 【 NetSec-Analyst 】 for free download on □ www.pdfvce.com □ □Authentic NetSec-Analyst Exam Hub
- NetSec-Analyst Dump File □ NetSec-Analyst Actual Braindumps □ Frenquent NetSec-Analyst Update □ Open ✔ www.testkingpass.com □✔□ enter 「 NetSec-Analyst 」 and obtain a free download □NetSec-Analyst Latest Test Vce
- Valid NetSec-Analyst Exam Duration □ NetSec-Analyst Actual Braindumps □ Real NetSec-Analyst Torrent □ Open 《 www.pdfvce.com 》 and search for [NetSec-Analyst] to download exam materials for free □NetSec-Analyst Valid Exam Pdf
- 2026 Updated Valid NetSec-Analyst Exam Tips | 100% Free Palo Alto Networks Network Security Analyst Detailed Answers □ Go to website [www.pdfdumps.com] open and search for □ NetSec-Analyst □ to download for free □ □NetSec-Analyst Actual Braindumps
- socials360.com, socialbuzzfeed.com, lawsonbrxb693899.wikisona.com, saadfxgr529694.tusblogos.com, bookmarkalexa.com, annieqtio430809.blogcudinti.com, safiyanbqd206423.tnpwiki.com, zaynabyobt527831.blogunteer.com, ineseqbo672015.anchor-blog.com, aushdc.com, Disposable vapes

2026 Latest CramPDF NetSec-Analyst PDF Dumps and NetSec-Analyst Exam Engine Free Share: https://drive.google.com/open?id=1BQQf4Dmc1ruFzL2XwNQvQfDUbrqt6JAl