

New NetSec-Analyst Exam Experience & NetSec-Analyst Dumps Questions



If you are interested in Dumpcollection's training program about Palo Alto Networks certification NetSec-Analyst exam, you can first on WWW.Dumpcollection.COM to free download part of the exercises and answers about Palo Alto Networks Certification NetSec-Analyst Exam as a free try. We will provide one year free update service for those customers who choose Dumpcollection's products.

Dumpcollection Palo Alto Networks Network Security Analyst (NetSec-Analyst) PDF exam questions file is portable and accessible on laptops, tablets, and smartphones. This pdf contains test questions compiled by experts. Answers to these pdf questions are correct and cover each section of the examination. You can even use this format of Palo Alto Networks Network Security Analyst questions without restrictions of place and time. This Palo Alto Networks NetSec-Analyst Pdf Format is printable to read real questions manually. We update our pdf questions collection regularly to match the updates of the Palo Alto Networks NetSec-Analyst real exam.

>> [New NetSec-Analyst Exam Experience](#) <<

Newest New NetSec-Analyst Exam Experience & Complete NetSec-Analyst Dumps Questions & Free Download Valid NetSec-Analyst Exam Papers

We even guarantee our customers that they will pass Palo Alto Networks NetSec-Analyst exam easily with our provided study material and if they failed to do it despite all their efforts they can claim a full refund of their money (terms and conditions apply). The

third format is the desktop software format which can be accessed after installing the software on your Windows computer or laptop. The Palo Alto Networks Network Security Analyst (NetSec-Analyst) has three formats so that the students don't face any serious problems and prepare themselves with fully focused minds.

Palo Alto Networks NetSec-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> 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 2	<ul style="list-style-type: none"> 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 3	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.

Palo Alto Networks Network Security Analyst Sample Questions (Q38-Q43):

NEW QUESTION # 38

A security analyst is investigating a persistent issue where an internal server, running a custom application over a non-standard TCP port (e.g., TCP 12345), cannot establish outbound connections to an external cloud service. The Palo Alto Networks firewall is configured with a security policy allowing this traffic with 'Application: any' and 'Service: application-default'. Packet captures show the initial SYN from the server, but no response from the cloud service. The firewall's traffic logs for this session show 'deny' with 'reason: untrusted' and 'action: drop'. What is the most plausible and complex reason for this behavior, indicating a deep understanding of App-ID and security profiles?

- A. The firewall's decryption profile is misconfigured for the outbound traffic, causing the 'untrusted' verdict.
- B. The external cloud service's IP address is mistakenly included in a custom URL category or External Dynamic List that is blocked by another policy.
- C. A custom threat signature is misfiring on the initial SYN packet, classifying it as malicious before App-ID can properly identify the application.
- D. The 'Service: application-default' setting is problematic because App-ID requires initial packets to establish a known application before allowing traffic, and for this non-standard port, it's failing classification or hitting a default security profile action.**
- E. The security policy rule for the internal server's outbound traffic is incorrectly placed after a default deny rule.

Answer: D

Explanation:

The critical details are 'non-standard TCP port', 'Application: any', 'Service: application-default', 'deny', and 'reason: untrusted'. When 'Service: application-default' is used with 'Application: any', the firewall attempts to identify the application. If it cannot, or if the initial packets don't conform to any known application on that port, it might hit a 'default-security-profile' (or a profile applied by a general rule) that has an 'action: reset-client' or 'drop' for 'unknown' or 'incomplete' application states. The 'untrusted' reason often comes from a security profile (like Antivirus, Anti-Spyware, Vulnerability Protection) applying a verdict. For a non-standard port, App-ID might struggle, leading to the session being marked as 'incomplete' or 'unknown', and thus subsequently acted upon by a security profile which defaults to 'untrusted' for unclassified or suspicious flows. This is a complex interaction between App-ID, Service definition, and Security Profiles for non-standard traffic. Option A would typically show 'deny' but not necessarily 'untrusted'. Option B would show a URL filtering block, not 'untrusted' for the initial SYN. Option D is possible but less likely given 'untrusted' rather than a decryption error. Option E is less likely for an initial SYN packet before any data payload, although not impossible.

NEW QUESTION # 39

Which Security profile would you apply to identify infected hosts on the protected network using DNS traffic?

- A. URL traffic
- B. vulnerability protection
- **C. anti-spyware**
- D. antivirus

Answer: C

NEW QUESTION # 40

Which plane on a Palo alto networks firewall provides configuration logging and reporting functions on a separate processor?

- **A. management**
- B. network processing
- C. security processing
- D. data

Answer: A

NEW QUESTION # 41

When is an event displayed under threat logs?

- A. Every time the firewall drops a connection
- **B. When traffic matches a corresponding Security Profile**
- C. When traffic matches any Security policy
- D. Every time a session is blocked

Answer: B

Explanation:

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/threat-logs#:~:text=Threat%20logs%20display%20entries%20when,security%20rule%20on%20the%20firewall.>

NEW QUESTION # 42

Given the topology, which zone type should zone A and zone B to be configured with?

□

- A. Tap
- B. Layer2
- **C. Layer3**
- D. Virtual Wire

Answer: C

NEW QUESTION # 43

With our Palo Alto Networks NetSec-Analyst study materials, you can make full use of those time originally spent in waiting for the delivery of exam files so that you can get preparations as early as possible. There is why our Palo Alto Networks NetSec-Analyst learning prep exam is well received by the general public.

NetSec-Analyst Dumps Questions: https://www.dumpcollection.com/NetSec-Analyst_braindumps.html