

Valid NetSec-Analyst Exam Questions Pdf, Ensure to pass the NetSec-Analyst Exam



What's more, part of that ExamDiscuss NetSec-Analyst dumps now are free: https://drive.google.com/open?id=1yPre-HrDMknp66fEChpGWL_bhYwPsI

The education level of the country has been continuously improved. At present, there are more and more people receiving higher education, and even many college graduates still choose to continue studying in school. Getting the test NetSec-Analyst certification maybe they need to achieve the goal of the learning process, have been working for the workers, have more qualifications can they provide wider space for development. The NetSec-Analyst Study Materials can provide them with efficient and convenient learning platform so that they can get the certification as soon as possible in the shortest possible time.

Palo Alto Networks NetSec-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	<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 2	<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.
Topic 3	<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 4	<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.

NetSec-Analyst Exam Questions Pdf | Latest Palo Alto Networks NetSec-Analyst: Palo Alto Networks Network Security Analyst

To meet the needs of users, and to keep up with the trend of the examination outline, our NetSec-Analyst exam questions will provide customers with latest version of our products. Our company's experts are daily testing our NetSec-Analyst study guide for timely updates. So we solemnly promise the users, our products make every effort to provide our users with the Latest NetSec-Analyst Learning Materials. As long as the users choose to purchase our NetSec-Analyst exam preparation materials, there is no doubt that he will enjoy the advantages of the most powerful update.

Palo Alto Networks Network Security Analyst Sample Questions (Q317-Q322):

NEW QUESTION # 317

You receive notification about new malware that infects hosts through malicious files transferred by FTP.

Which Security profile detects and protects your internal networks from this threat after you update your firewall's threat signature database?

- A. Data Filtering profile applied to outbound Security policy rules.
- **B. Antivirus profile applied to inbound Security policy rules.**
- C. Vulnerability Protection profile applied to outbound Security policy rules.
- D. URL Filtering profile applied to inbound Security policy rules.

Answer: B

Explanation:

Reference:

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles>

NEW QUESTION # 318

Place the following steps in the packet processing order of operations from first to last.

□

Answer:

Explanation:

□

NEW QUESTION # 319

The CFO found a USB drive in the parking lot and decide to plug it into their corporate laptop. The USB drive had malware on it that loaded onto their computer and then contacted a known command and control (CnC) server, which ordered the infected machine to begin Exfiltrating data from the laptop.

Which security profile feature could have been used to prevent the communication with the CnC server?

- A. Create a security policy and enable DNS Sinkhole
- **B. Create an anti-spyware profile and enable DNS Sinkhole**
- C. Create an antivirus profile and enable DNS Sinkhole
- D. Create a URL filtering profile and block the DNS Sinkhole category

Answer: B

NEW QUESTION # 320

Which profile should be used to obtain a verdict regarding analyzed files?

- A. Vulnerability profile
- B. Advanced threat prevention
- **C. WildFire analysis**
- D. Content-ID

Answer: C

Explanation:

* A profile is a set of rules or settings that defines how the firewall performs a specific function, such as detecting and preventing threats, filtering URLs, or decrypting traffic¹.

* There are different types of profiles that can be applied to different types of traffic or scenarios, such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, Data Filtering, Decryption, or WildFire Analysis¹.

* The WildFire Analysis profile is a profile that enables the firewall to submit unknown files or email links to the cloud-based WildFire service for analysis and verdict determination². WildFire is the industry's most advanced analysis and prevention engine for highly evasive zero-day exploits and malware³. WildFire uses a variety of malware detection techniques, such as static analysis, dynamic analysis, machine learning, and intelligent run-time memory analysis, to identify and protect against unknown threats^{3,4}.

* The Vulnerability Protection profile is a profile that protects the network from exploits that target known software vulnerabilities. It allows the administrator to configure the actions and log settings for each vulnerability severity level, such as critical, high, medium, low, or informational⁵.

* Content-ID is not a profile, but a feature of the firewall that performs multiple functions to identify and control applications, users, content, and threats on the network. Content-ID consists of four components: App-ID, User-ID, Content Inspection, and Threat Prevention.

* Advanced Threat Prevention is not a profile, but a term that refers to the comprehensive approach of Palo Alto Networks to prevent sophisticated and unknown threats. Advanced Threat Prevention includes WildFire, but also other products and services, such as DNS Security, Cortex XDR, Cortex XSOAR, and AutoFocus.

Therefore, the profile that should be used to obtain a verdict regarding analyzed files is the WildFire Analysis profile.

References:

1: Security Profiles - Palo Alto Networks 2: WildFire Analysis Profile - Palo Alto Networks 3: WildFire - Palo Alto Networks 4: Advanced Wildfire as an ICAP Alternative | Palo Alto Networks 5: Vulnerability Protection Profile - Palo Alto Networks : [Content-ID - Palo Alto Networks] : [Advanced Threat Prevention - Palo Alto Networks]

NEW QUESTION # 321

A Security Operations Center (SOC) is leveraging Strata Cloud Manager (SCM) for centralized monitoring and incident response. They need to quickly identify firewalls experiencing high CPU utilization due to a recent brute-force attack attempt, and then apply a temporary security policy to block the offending IP addresses across multiple firewall groups. Which SCM capabilities facilitate this agile response?

- A. Next-Gen Firewall hardware refresh scheduling.
- B. Network Packet Broker integration for deep packet inspection.
- C. Automated Cortex XDR integration for endpoint remediation.
- **D. Real-time logging and reporting via SCM Analytics, coupled with centralized policy push.**
- E. Prisma Access Mobile User VPN configuration and monitoring.

Answer: D

Explanation:

SCM Analytics provides real-time visibility into firewall health and security events, allowing the SOC to identify high CPU utilization and attack patterns. Once identified, SCM's centralized policy management enables rapid creation and deployment of new security rules (e.g., blocking offending IPs) to multiple firewall groups simultaneously, significantly reducing response time during incidents.

NEW QUESTION # 322

.....

There are three versions of our NetSec-Analyst exam questions. And all of the PDF version, online engine and windows software of the NetSec-Analyst study guide will be tested for many times. Although it is not easy to solve all technology problems, we have excellent experts who never stop trying. And whenever our customers have any problems on our NetSec-Analyst Practice Engine, our experts will help them solve them at the first time.

New NetSec-Analyst Exam Testking: <https://www.examdisscuss.com/Palo-Alto-Networks/exam/NetSec-Analyst/>

- DOWNLOAD the newest ExamDiscuss NetSec-Analyst PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1yPrese-HrDMknp66fEChpGWL_bhYwPsI

DOWNLOAD the newest ExamDiscuss NetSec-Analyst PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1yPrese-HrDMknp66fEChpGWL_bhYwPsI