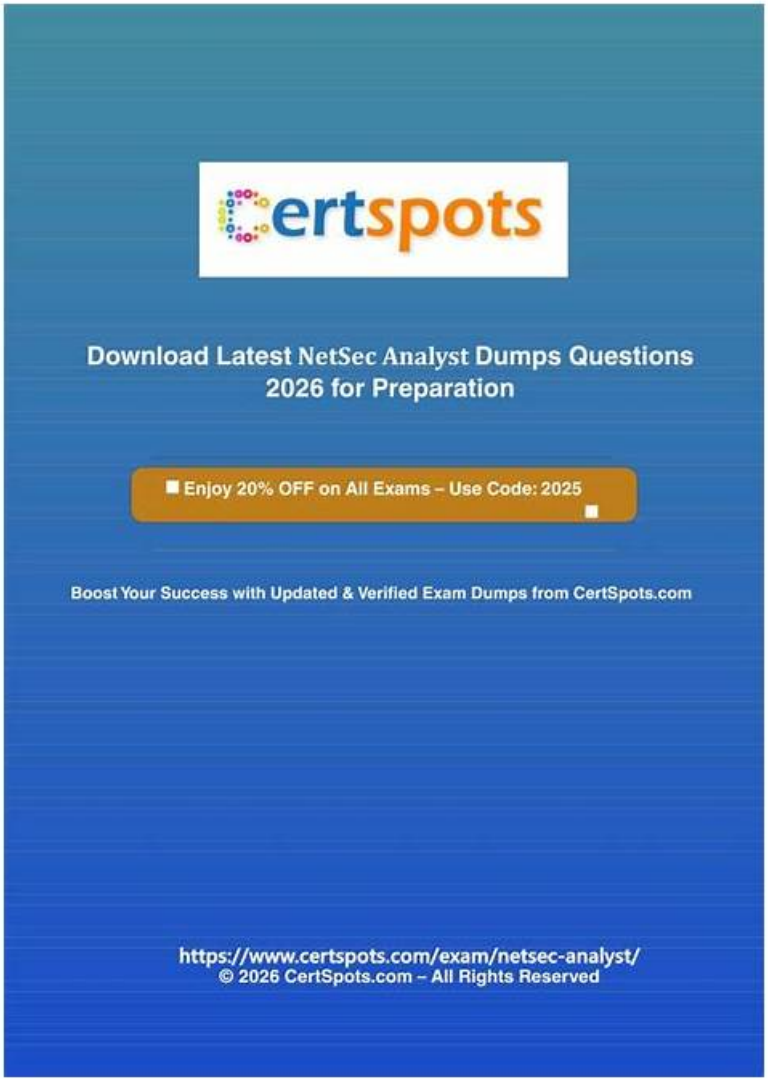
NetSec-Analyst Sample Questions Answers, New NetSec-Analyst Dumps Book



BTW, DOWNLOAD part of ExamPrepAway NetSec-Analyst dumps from Cloud Storage: https://drive.google.com/open?id=13VmRDZA7OjFUw7bZIBAP1u3iqGaMqNbQ

NetSec-Analyst training materials are famous for instant access to download, and you can receive your download link and password within ten minutes after payment. And if you don't, you don't receive, you can contact with us, we will resolve it for you. Besides, we offer free demo for you, we recommend you to have a try before buying NetSec-Analyst Training Materials. You can enjoy free update for 365 days if you choose us, so that you can obtain the latest information timely. And the latest version for NetSec-Analyst exam dumps will be sent to your email automatically. You just need to receive them,

Palo Alto Networks NetSec-Analyst Exam Syllabus Topics:

Topic	Details

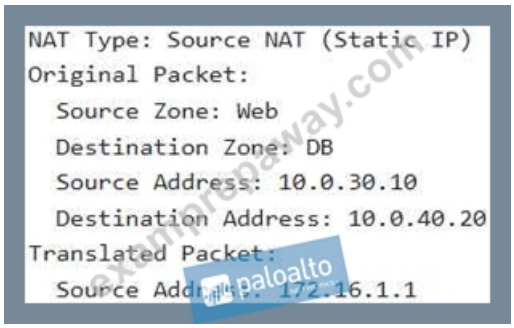
Topic 1	• Management and Operations: This section of the exam measures the skills of Security Operations Professionals and covers the use of centralized management tools to maintain and monitor firewall environments. It focuses on Strata Cloud Manager, folders, snippets, automations, variables, and logging 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 2	• 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 3	• 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 4	• 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.

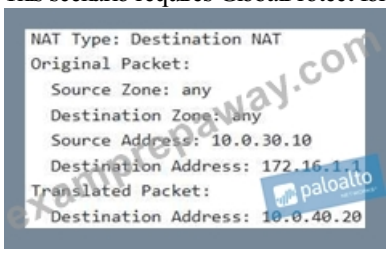
New NetSec-Analyst Dumps Book - Latest NetSec-Analyst Study Guide

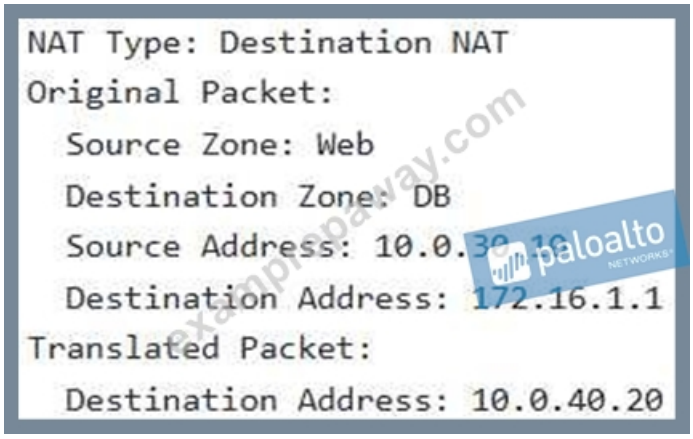
There are many merits of our product on many aspects and we can guarantee the quality of our Palo Alto Networks Network Security Analyst NetSec-Analyst practice engine. Firstly, our experienced expert team compile them elaborately based on the real exam. Secondly, both the language and the content of our Palo Alto Networks NetSec-Analyst Study Materials are simple.

Palo Alto Networks Network Security Analyst Sample Questions (Q103-Q108):

NEW QUESTION # 103
You are deploying a new application in a segmented network behind a Palo Alto Networks firewall. The application consists of a web frontend (10.0.30.10) in the 'Web' zone and a database backend (10.0.40.20) in the 'DB' zone. The web frontend needs to connect to the database. Due to a legacy application requirement, the web frontend is hardcoded to connect to 'db.internal.com', which resolves to 172.16.1.1. You cannot reconfigure the web application. Your task is to use NAT to redirect traffic from 10.0.30.10 destined for 172.16.1.1 to the actual database server at 10.0.40.20. Which of the following NAT policy configurations would correctly achieve this, assuming appropriate security policies exist?

- A. 

- B. This scenario requires GlobalProtect for VPN-based access to the database, not NAT.
- C. 

- D. NAT Type: Destination NAT
Original Packet:
Source Zone: Web
Destination Zone: any
Source Address: 10.0.30.10
Destination Address: 172.16.1.1
Translated Packet:
Destination Address: 10.0.40.20
- E. 

Answer: E

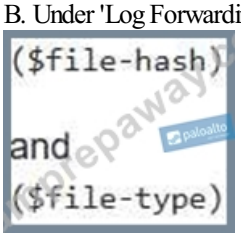
Explanation:
The core problem is that the web frontend sends traffic to a 'dummy' IP (172.16.1.1) that needs to be redirected to the actual database IP (10.0.40.20). This is a classic use case for Destination NAT (DNAT). The firewall needs to intercept packets from 10.0.30.10 going to 172.16.1.1 and change their destination to 10.0.40.20.
Let's break down Option A:
- NAT Type: Destination NAT: Correct, as we are changing the destination of the packet.
- Original Packet: This describes what the firewall sees coming in. The source is 10.0.30.10 (from the 'Web' zone), and it's trying to reach 172.16.1.1, with the intent to go to the 'DB' zone. So, Source Zone: Web, Destination Zone: DB, Source Address: 10.0.30.10, Destination Address: 172.16.1.1 are all correct.
- Translated Packet: This describes how the firewall changes the packet. We want the destination to become 10.0.40.20. So, Translated Destination Address: 10.0.40.20 is correct.
Options C and D are less specific ('any' for destination zone or source/destination zone), which might lead to unintended NAT for other traffic.
Option B is a Source NAT, which changes the source IP, not the destination, and is completely incorrect for this scenario. Option E is irrelevant.

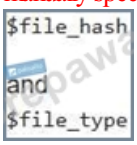
NEW QUESTION # 104
Identify the correct order to configure the PAN-OS integrated USER-ID agent.
3. add the service account to monitor the server(s)
2. define the address of the servers to be monitored on the firewall
4. commit the configuration, and verify agent connection status
1. create a service account on the Domain Controller with sufficient permissions to execute the User- ID agent

- A. 1-4-3-2
- B. 3-1-2-4
- C. 2-3-4-1
- D. 1-3-2-4

Answer: D

NEW QUESTION # 105
A Palo Alto Networks firewall has a Log Forwarding Profile configured to send all logs to a syslog server. The security team needs to monitor 'wildfire' verdicts in real-time. To facilitate this, they request that the forwarded 'wildfire' logs include additional custom fields that are not part of the default syslog format. Specifically, they need the 'file-hash' and 'file-type' from WildFire logs to be explicitly included. How can this be achieved within the Log Forwarding Profile configuration?

- A. Within the Log Forwarding Profile, select 'WildFire' log type. Under 'Syslog Fields', you can add custom fields. For 'Field Name', enter 'file-hash' and for 'Value', use the predefined variable for file hash. Repeat for 'file-type'.
- B. Under 'Log Forwarding Profile > Syslog Server > Custom Log Format', use


- C. In the Log Forwarding Profile, configure the syslog destination to use 'Custom Log Format'. Then, in the format string, manually specify the desired fields using predefined variables. For WildFire logs, this would include variables like


- D. Under 'Log Forwarding Profile > Syslog Server > CEF Format', enable the 'WildFire' log type and then add new custom entries under 'Custom Fields' for 'file- hash' and 'file-type'.
- E. In the Log Forwarding Profile, you cannot add custom fields to existing log types like WildFire. This functionality is only available for User-ID mapping or custom applications.

Answer: C

Explanation:
Option E is the correct approach. Palo Alto Networks firewalls allow extensive customization of log formats when using a 'Custom Log Format' in a Log Forwarding Profile. For each log type, you can define a string using a combination of static text and predefined variables (e.g., '$src', '$dst', '$app' , and crucially, specific fields like '$file_hasm and '$file_type' for WildFire logs). Option A uses slightly incorrect variable syntax but is conceptually close. Option B is incorrect as custom fields are indeed possible for log types. Option C (CEF) uses a standard format, and while it's extensible, directly adding arbitrary custom fields for existing log types as suggested isn't the primary method for adding these specific fields. Option D points to 'Syslog Fields' but that's typically for remapping or adding a few standard fields, not for defining the entire custom format with specific variables.

NEW QUESTION # 106
A secure healthcare network leverages Palo Alto Networks NGFWs to protect critical medical IoT devices (IoMT) like infusion pumps and patient monitors. These devices communicate using proprietary protocols over TCP. The security team has identified that some of these devices are attempting to establish undocumented SSH connections to external IP addresses, likely due to a compromise. The challenge is that the NGFW's 'Application-ID' correctly identifies the proprietary IoMT application, but it also identifies the rogue SSH connection from the same device . How can the security policy, leveraging IoT security profiles, be configured to allow the legitimate IoMT proprietary application while blocking the specific SSH connection from the compromised

device without disrupting essential medical operations?

- A. Configure an 'IoT Security Profile' with 'Application Function Filtering' to disable all functions of the proprietary IoMT application, effectively blocking all communication.
- B. Utilize 'Application Filters' to create a 'Permitted-IoMT-Apps' group including only the proprietary IoMT application. Create a 'Security Policy' rule allowing only this 'Permitted-IoMT-Apps' group from the IoMT device group, effectively denying other applications like SSH.
- C. Implement 'Application Override' for the proprietary IoMT application's port, forcing all traffic on that port to be identified as the legitimate IoMT app, thereby preventing SSH from being identified.
- D. Create a 'Security Policy' rule with 'Source: Compromised-IoMT-Device-Group', 'Destination: Any', 'Application: ssh', 'Action: Deny'. Place this rule above the general 'Allow' rule for IoMT devices.
- E. Apply an 'Anti-Spyware' profile to the IoMT security policy with a custom signature for the specific SSH traffic pattern observed from the compromised device.

Answer: D

Explanation:
Option A is the most effective and precise solution. Palo Alto Networks' 'Application-ID' works by identifying applications regardless of port. If both the proprietary IoMT app and SSH are identified from the same device, the most direct way to block SSH while allowing the legitimate app is to create a specific 'deny' rule for SSH, targeted at the compromised device (or device group), and place it higher in the rulebase than any 'allow' rule for that device/group. Since firewall rules are processed top-down, the deny for SSH will be hit first. Option B is incorrect as it would block all legitimate IoMT functions. Option C (Anti-Spyware with custom signature) is a reactive measure for known threats; policy-based blocking is more direct for application control. Option D (Application Override) is a misapplication; it would force all traffic on the IoMT port to be seen as the IoMT app, potentially masking the rogue SSH if it uses the same port, or preventing accurate identification if SSH uses a different port. Application-ID is already correctly identifying both. Option E is a good general practice for 'least privilege' (allowing only known applications), but Option A specifically addresses the immediate need to block the identified SSH from the compromised device without affecting the legitimate IoMT app.

NEW QUESTION # 107
An administrator manages a network with 300 addresses that require translation. The administrator configured NAT with an address pool of 240 addresses and found that connections from addresses that needed new translations were being dropped.
Which type of NAT was configured?

- A. Dynamic IP
- B. Dynamic IP and Port
- C. Static IP
- D. Destination NAT

Answer: A

Explanation:
The size of the NAT pool should be equal to the number of internal hosts that require address translations. By default, if the source address pool is larger than the NAT address pool and eventually all of the NAT addresses are allocated, new connections that need address translation are dropped. To override this default behavior, use Advanced (Dynamic IP/Port Fallback) to enable the use of DIPP addresses when necessary

NEW QUESTION # 108
.....

Download ☀ NetSec-Analyst □☀□ for free by simply entering ➠ www.prepawayexam.com □ website □Valid Exam NetSec-Analyst Practice

- New NetSec-Analyst Test Vce □ NetSec-Analyst Valid Dump □ Exam NetSec-Analyst Labs □ Easily obtain ⇛ NetSec-Analyst ⇚ for free download through ✔ www.pdfvce.com □✔□ □Detailed NetSec-Analyst Answers
- New NetSec-Analyst Test Vce □ Valid NetSec-Analyst Exam Answers □ Exam NetSec-Analyst Labs □ Enter □ www.troytecdumps.com □ and search for ☀ NetSec-Analyst □☀□ to download for free □New NetSec-Analyst Test Vce
- Palo Alto Networks NetSec-Analyst Realistic Sample Questions Answers Free PDF Quiz ➡□ Easily obtain （ NetSec-Analyst ） for free download through ➠ www.pdfvce.com □ □NetSec-Analyst Certificate Exam
- NetSec-Analyst Pdf Pass Leader □ Real NetSec-Analyst Exam Dumps □ NetSec-Analyst Reliable Test Syllabus ↪ Open website “ www.dumpsquestion.com ” and search for “ NetSec-Analyst ” for free download □NetSec-Analyst Torrent
- Latest NetSec-Analyst Exam Guide □ Exam NetSec-Analyst Pattern □ Exam NetSec-Analyst Labs □ Immediately open [www.pdfvce.com] and search for □ NetSec-Analyst □ to obtain a free download □NetSec-Analyst Accurate Study Material
- Palo Alto Networks NetSec-Analyst Realistic Sample Questions Answers Free PDF Quiz □ Download [NetSec-Analyst] for free by simply searching on 「 www.pdfdumps.com 」 □Latest NetSec-Analyst Exam Guide
- NetSec-Analyst Torrent □ NetSec-Analyst Accurate Study Material □ NetSec-Analyst Latest Study Guide □ Open [www.pdfvce.com] and search for ➤ NetSec-Analyst □ to download exam materials for free □Exam NetSec-Analyst Voucher
- NetSec-Analyst Reliable Test Syllabus □ NetSec-Analyst Accurate Study Material □ Exam NetSec-Analyst Pattern □ □ Enter ➽ www.validtorrent.com □ and search for { NetSec-Analyst } to download for free □NetSec-Analyst Valid Test Registration
- New NetSec-Analyst Dumps Pdf ✡ Latest NetSec-Analyst Exam Guide □ NetSec-Analyst Latest Study Guide □ Download “ NetSec-Analyst ” for free by simply entering ▸ www.pdfvce.com ◂ website □New NetSec-Analyst Test Vce
- Pass Guaranteed Quiz NetSec-Analyst - Palo Alto Networks Network Security Analyst –Efficient Sample Questions Answers □ Download 【 NetSec-Analyst 】 for free by simply entering □ www.testkingpass.com □ website □NetSec-Analyst Valid Test Registration
- 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, 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, elearning.eauqardho.edu.so, ncon.edu.sa, www.stes.tyc.edu.tw, lms.ait.edu.za, Disposable vapes

2026 Latest ExamPrepAway NetSec-Analyst PDF Dumps and NetSec-Analyst Exam Engine Free Share: https://drive.google.com/open?id=13VmRDZA7OjFUw7bZIBAP1u3iqGaMqNbQ