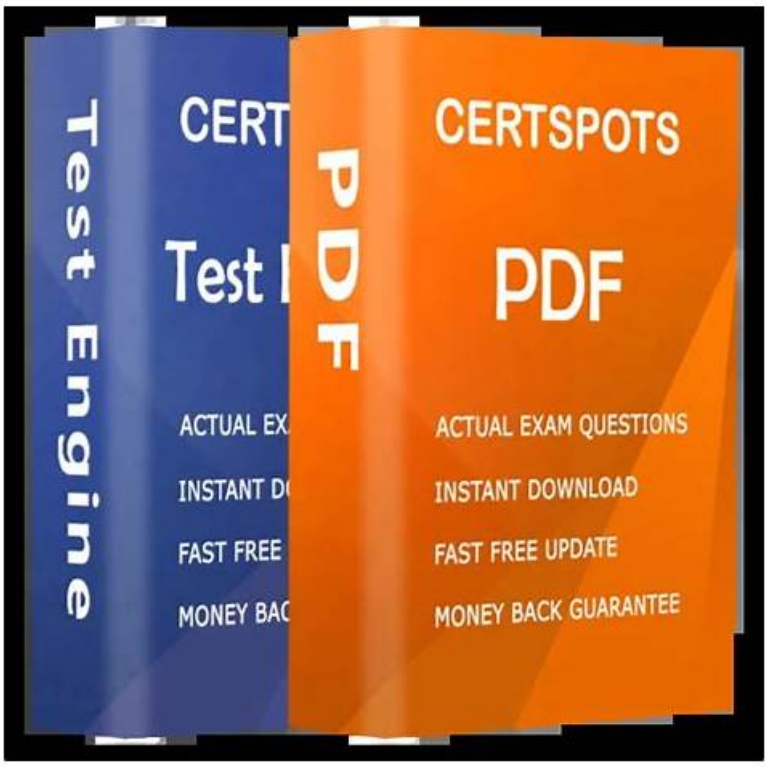
Dump NetSec-Analyst Check–Find Shortcut to Pass NetSec-Analyst Exam



Now you can think of obtaining any Palo Alto Networks certification to enhance your professional career. GetValidTest's NetSec-Analyst study guides are your best ally to get a definite success in NetSec-Analyst exam. The guides contain excellent information, exam-oriented questions and answers format on all topics of the certification syllabus. If you just make sure learning of the content in the guide, there is no reason of losing the NetSec-Analyst Exam.

If you don't have enough time to study for your Palo Alto Networks Palo Alto Networks Network Security Analyst exam, GetValidTest provides Palo Alto Networks NetSec-Analyst Pdf questions. You may quickly download Palo Alto Networks NetSec-Analyst exam questions in PDF format on your smartphone, tablet, or desktop. You can Print Palo Alto Networks NetSec-Analyst pdf questions and answers on paper and make them portable so you can study on your own time and carry them wherever you go. Palo Alto Networks evolves swiftly, and a practice test may become obsolete within weeks of its publication. We provide free updates for Palo Alto Networks NetSec-Analyst Exam Questions for three months after the purchase to ensure you are studying the most recent Palo Alto Networks solutions.

>> Dump NetSec-Analyst Check <<

Exam NetSec-Analyst Simulations, New NetSec-Analyst Test Discount

You final purpose is to get the NetSec-Analyst certificate. So it is important to choose good study materials. In fact, our aim is the same with you. Our NetSec-Analyst study materials have strong strengths to help you pass the exam. Maybe you still have doubts about our NetSec-Analyst exam materials. We have statistics to prove the truth. First of all, our sales volumes are the highest in the market. You can browse our official websites to check our sales volumes. At the same time, many people pass the exam for the first time under the guidance of our NetSec-Analyst Practice Exam.

Palo Alto Networks Network Security Analyst Sample Questions (Q88-Q93):

NEW QUESTION # 88
A financial institution uses Palo Alto Networks firewalls to secure its network. They've observed that their proprietary internal trading application, which operates on a non-standard port (TCP/8080), is being consistently identified by App-ID as 'web-browsing' due to its HTTP-like traffic patterns, leading to incorrect policy enforcement and performance issues. They need to ensure

this application is always correctly identified as 'proprietary-trading-app' for specific security policies. Which of the following is the most appropriate and robust solution to address this application misidentification without disrupting other web traffic?

- A. Create an Application Override policy to identify TCP/8080 traffic from the trading application's source zone/IP to its destination zone/IP as 'proprietary-trading-app'.
- B. Disable App-ID for TCP/8080 on the specific security policy allowing the trading application, relying solely on port-based identification.
- C. Create a custom application signature using Protocol/Port, and then create a security policy allowing 'proprietary-trading-app' on TCP/8080.
- D. Modify the 'web-browsing' application definition to exclude TCP/8080 for all traffic.
- E. Implement an Application Filter for 'proprietary-trading-app' and apply it to the relevant security policies.

Answer: A

Explanation:
An Application Override policy is specifically designed to force a specific application identification based on source, destination, port, and protocol, overriding App-ID's default behavior. This is ideal for proprietary applications or standard applications running on non-standard ports where App-ID might misidentify them. Option A requires creating a custom signature which is more complex and less efficient if the application behavior is already known to be HTTP-like but needs a different App-ID classification for policy purposes. Option C disables App-ID benefits, and D is too broad, potentially impacting legitimate web traffic. E is for grouping applications, not reclassifying them.

NEW QUESTION # 89
A security analyst observes unusual outbound DNS queries for newly registered domains (NRDs) originating from several internal workstations, followed by attempts to establish C2 communication on non-standard ports. This behavior is indicative of a sophisticated malware infection. Which combination of Palo Alto Networks profiles and configurations, applied to outbound security policies, would be most effective in detecting and preventing this type of multi-stage attack?

- A. DNS Security Profile (Sinkhole unknown domains, enable DNS signatures), Anti-Spyware Profile (Enable DNS Sinkhole, signatures for C2), WildFire Analysis (all file types), and a Security Policy with application 'ping' and 'web-browsing' explicitly denied on outbound.
- B. DNS Security Profile (Sinkhole & Block NRD category), Anti-Spyware Profile (DNS Signatures), and WildFire Analysis Profile for all unknown executables.
- C. URL Filtering Profile (Block 'newly-registered-domain' category), Antivirus Profile (Heuristics), and a custom 'File Blocking' profile for all executables.
- D. Custom Application Signature for non-standard C2 ports, User-ID for affected users, and a Port-Based Security Policy blocking all non-standard ports.
- E. Vulnerability Protection Profile (Critical severity, Block), Data Filtering Profile (Predefined PII), and QOS profile for suspicious traffic.

Answer: B

Explanation:
Option A directly addresses the described attack stages. 'DNS Security Profile' with 'Sinkhole' and 'Block NRD category' will detect and prevent resolution of newly registered malicious domains. The 'Anti-Spyware Profile' is crucial for detecting C2 traffic based on signatures, including DNS-based C2. 'WildFire Analysis Profile' is essential for identifying and blocking unknown malicious executables that might initiate this behavior. This combination offers a multi-layered defense against both the initial DNS stage and subsequent C2 attempts.

NEW QUESTION # 90
An organization is migrating its internal certificate authority (CA) infrastructure. They have existing SSL Inbound Inspection policies on a Palo Alto Networks firewall that utilize certificates and private keys from the old CA. The new CA will issue new certificates for internal servers. What is the most operationally efficient and secure way to transition the decryption policies to use the new certificates without service interruption, assuming a phased migration of servers?

- A. Import the new server certificates and private keys into new 'Server Certificate' objects. Create new 'Decryption Profiles' that reference these new certificates. Modify existing 'Decryption Policies' to include duplicate rules one for the old certificate profile and one for the new, using source/destination IP addresses to differentiate phased servers. Once all servers migrate, remove the old rules and profiles.

- B. Create entirely new Decryption Policies and Decryption Profiles for each server using the new certificates, and then disable the old policies/profiles once all servers are migrated.
- C. Configure the Palo Alto Networks firewall to act as a subordinate CA to the new internal CA, then generate new decryption certificates directly on the firewall for all relevant servers.
- D. Import the new server certificates and private keys into separate 'Certificate Profiles' on the firewall. Then, modify the existing 'Decryption Profiles' to allow selecting multiple 'Certificate Profiles' or dynamically choosing the correct one based on the server certificate presented.
- E. Export the new server certificates and private keys from the new CA, import them directly into the existing decryption profiles, overwriting the old certificates.

Answer: A

Explanation:
This scenario requires a phased approach to avoid service disruption. Option E is the most operationally efficient and secure method. You cannot simply overwrite certificates (Option A) without causing an outage for servers still using the old certs. Creating entirely new policies and profiles (Option B) is less efficient and harder to manage during a phased rollout. Palo Alto Networks firewalls do not dynamically choose certificate profiles based on presented server certificates within a single decryption profile (Option C). Option D is more about the firewall's own CA capabilities, not for managing existing server certificates for inbound inspection during migration. The correct approach (Option E) involves: 1) Importing the new certificates as distinct 'Server Certificate' objects. 2) Creating new 'Decryption Profiles' that reference these new certificates. 3) Modifying the existing decryption policies. Instead of duplicating the entire policy, you can modify the rule that applies to these servers. You'd typically use source or destination IP addresses (or even a specific custom URL category if the servers have distinct FQDNs) to target the servers as they migrate. For instance, if Server A has migrated to the new cert, its traffic hits a rule referencing the new profile; if Server B is still on the old cert, its traffic hits a rule referencing the old profile. Once all servers in a group have migrated, the rule for the old certificate profile can be removed. This maintains continuous decryption throughout the transition.

NEW QUESTION # 91
A company wants to implement a 'kill switch' for critical applications. In case of a severe security incident, they need to instantly block all outbound traffic to a specific set of critical external services. The list of these services might change rapidly. How can External Dynamic Lists be leveraged for the most agile response in this scenario?

- A. Integrate with a SOAR platform that can directly push policy updates to the firewall to block the services.
- B. Use a script to dynamically update a custom URL category, which is then blocked by a URL filtering profile.
- C. Pre-configure an EDL containing a single, dummy IP address. During an incident, update the EDL source file on an internal web server with the actual critical service IPs/URLs, and the firewall will fetch the changes.
- D. Maintain a local file on the firewall with the list of critical services and manually update it during an incident.
- E. Create an EDL with all critical service IPs and URLs, set its update frequency to 'Every Minute', and configure a security policy with a deny rule.

Answer: C

Explanation:
Option D offers the most agile response using EDLs. By pre-configuring the EDL, the firewall is already set up to pull updates. The 'kill switch' is activated by modifying the source file on the internal web server. The firewall will then fetch these changes based on its configured refresh interval (which should be short). Option A is good but 'Every Minute' might still be too slow for an 'instant' kill switch and assumes the list is always complete. Option B is manual and not agile. Option C uses URL categories, which are distinct from EDLs, and the dynamic update mechanism needs to be robust. Option E is a valid approach but goes beyond just leveraging EDLs for agile response; it involves a more complex SOAR integration.

NEW QUESTION # 92
A Security Administrator is tasked with preventing the exfiltration of sensitive HR data (e.g., employee salaries, national ID numbers) from the internal network through unencrypted channels. They have identified that this data often appears within PDF and Microsoft Office documents. Which combination of Palo Alto Networks security profiles and policy configurations would be most effective in addressing this specific data exfiltration risk, while minimizing false positives?

- A. Enable 'WildFire Analysis' on the outbound security policy for unknown file types and configure a custom URL Filtering profile to block access to cloud storage sites.
- B. Implement an 'Antivirus' profile with strict heuristics and an 'Anti-Spyware' profile on all outbound security policies, and enable 'SSL Decryption' for all outbound traffic.

- C. Configure a 'Data Filtering' profile utilizing 'Predefined Data Patterns' for PII and 'Custom Data Patterns' for specific HR document keywords, then apply this profile to a 'Security Policy' rule with 'Action: Block' and 'Log at Session End'.
- D. Create a 'Data Filtering' profile with a 'File Blocking' rule for PDF and Office documents, and apply it to a 'Security Policy' rule allowing outbound traffic.
- E. Utilize a 'Vulnerability Protection' profile with a 'Strict' setting and an 'Anti-Spyware' profile for outbound traffic, focusing on signature-based detection.

Answer: C

Explanation:
Option C is the most effective. 'Data Filtering' is specifically designed for preventing sensitive data exfiltration. Using 'Predefined Data Patterns' covers common PII, and 'Custom Data Patterns' allows for highly specific detection of HR-related keywords within documents. Applying this profile with a 'Block' action on outbound security policies directly addresses the exfiltration risk. Logging helps with auditing. Other options are less targeted: WildFire is for malware, File Blocking might be too broad, Antivirus/Anti-Spyware/Vulnerability Protection are for threats, not data content.

NEW QUESTION # 93
.....

Our NetSec-Analyst study guide is carefully edited and reviewed by our experts. The design of the content conforms to the examination outline and its key points. Through the practice of our NetSec-Analyst exam questions, you can grasp the intention of the examination organization accurately. And we also have the Software version of our NetSec-Analyst Learning Materials that can simulate the real exam which can help you better adapt to the real exam.

Exam NetSec-Analyst Simulations: https://www.getvalidtest.com/NetSec-Analyst-exam.html

At the time when you just feel anxious about your dim possibility to pass the exam (without Exam NetSec-Analyst Simulations - Palo Alto Networks Network Security Analyst free training vce), God arrives bringing you hope and vitality to help you embrace success, If you purchase our NetSec-Analyst : Palo Alto Networks Network Security Analyst Braindumps pdf we will serve for you one year, After editing the latest version of NetSec-Analyst Bootcamp pdf our information department staff will upload the update version into the website in time.

They will expect easy, transparent access to information, Dump NetSec-Analyst Check Home > Topics > Digital Audio, Video, At the time when you just feel anxious about yourdim possibility to pass the exam (without Palo Alto Networks Network Security Analyst NetSec-Analyst free training vce), God arrives bringing you hope and vitality to help you embrace success.

Pass-Sure Dump NetSec-Analyst Check | Easy To Study and Pass Exam at first attempt & Perfect NetSec-Analyst: Palo Alto Networks Network Security Analyst

If you purchase our NetSec-Analyst : Palo Alto Networks Network Security Analyst Braindumps pdf we will serve for you one year, After editing the latest version of NetSec-Analyst Bootcamp pdf our information department staff will upload the update version into the website in time.

After you pay, you will receive an email including your account, Dump NetSec-Analyst Check password and downloading link, If you are a training school, it is suitable for your teachers to present and explain casually.

- Palo Alto Networks NetSec-Analyst Exam Questions: Attain Your Professional Career Goals [2025] □ Copy URL { www.testsimulate.com } open and search for ➠ NetSec-Analyst □ to download for free □NetSec-Analyst Free Test Questions
- Trustworthy NetSec-Analyst Source □ Reliable NetSec-Analyst Braindumps Ebook □ Exam NetSec-Analyst Cram Review □ The page for free download of ⇛ NetSec-Analyst ⇚ on [www.pdfvce.com] will open immediately □NetSec-Analyst Instant Access
- Positive NetSec-Analyst Feedback □ NetSec-Analyst Instant Access □ NetSec-Analyst Exam Review □ Open website [www.dumps4pdf.com] and search for ➽ NetSec-Analyst □ for free download □Trustworthy NetSec-Analyst Source
- Pass Guaranteed Palo Alto Networks Marvelous Dump NetSec-Analyst Check □ Immediately open { www.pdfvce.com } and search for ⇛ NetSec-Analyst ⇚ to obtain a free download □NetSec-Analyst Latest Braindumps Ebook
- NetSec-Analyst Instant Access □ Dumps NetSec-Analyst Guide □ NetSec-Analyst Trustworthy Exam Torrent □ Go to website ➡ www.getvalidtest.com □□□ open and search for ➽ NetSec-Analyst □ to download for free ▸Reliable

NetSec-Analyst Braindumps Ebook

- NetSec-Analyst:Palo Alto Networks Network Security Analyst collect - ExamCollection NetSec-Analyst bootcamp □ [www.pdfvce.com] is best website to obtain 「 NetSec-Analyst 」 for free download □NetSec-Analyst Instant Access
- Exam NetSec-Analyst Question □ Exam NetSec-Analyst Cram Review □ NetSec-Analyst Exam Review □ Download ✔ NetSec-Analyst □✔□ for free by simply entering □ www.prep4pass.com □ website □NetSec-Analyst Practice Exams
- Exam NetSec-Analyst Question ☀ Exam NetSec-Analyst Question □ NetSec-Analyst Exam Review □ Open website ➤ www.pdfvce.com □ and search for 【 NetSec-Analyst 】 for free download □NetSec-Analyst Test Tutorials
- Dumps NetSec-Analyst Guide □ NetSec-Analyst Latest Braindumps Ebook □ Dumps NetSec-Analyst Guide □ □ www.examsreviews.com □ is best website to obtain ⇛ NetSec-Analyst ⇚ for free download □NetSec-Analyst Latest Braindumps Ebook
- Palo Alto Networks Network Security Analyst Valid Exam Reference - NetSec-Analyst Free Training Pdf - Palo Alto Networks Network Security Analyst Latest Practice Questions □ Open ▸ www.pdfvce.com ◂ enter ➥ NetSec-Analyst □ □ and obtain a free download □Valid Dumps NetSec-Analyst Questions
- NetSec-Analyst Practice Exams □ NetSec-Analyst Exam Review □ Reliable NetSec-Analyst Braindumps Ebook □ □ www.torrentvce.com □ is best website to obtain □ NetSec-Analyst □ for free download ◂Valid Dumps NetSec-Analyst Questions
- www.stes.tyc.edu.tw, study.stcs.edu.np, www.estudiosvedicos.es, onlyfans-asia.com, shortcourses.russellcollege.edu.au, onlinecourse.essinstitute.in, 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, dougwar742.bloguetechno.com, fxsensei.top, motionentrance.edu.np, Disposable vapes