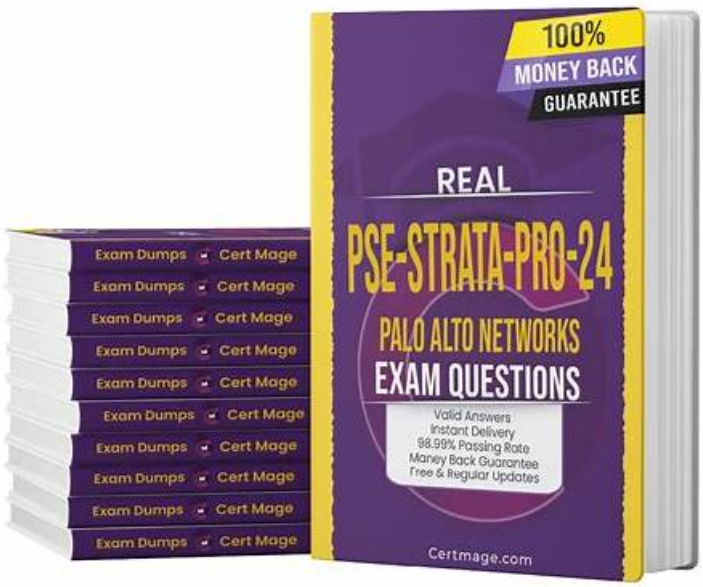
Palo Alto Networks PSE-Strata-Pro-24 Reliable Dumps & PSE-Strata-Pro-24 Accurate Prep Material



BTW, DOWNLOAD part of TestInsides PSE-Strata-Pro-24 dumps from Cloud Storage: https://drive.google.com/open?id=1BzEYIZcsBn602JB9oZz5cSH1FOHPIYv8

Keep reading because we have discussed specifications of Palo Alto Networks Systems Engineer Professional - Hardware Firewall PSE-Strata-Pro-24 PDF format, desktop Palo Alto Networks Systems Engineer Professional - Hardware Firewall PSE-Strata-Pro-24 practice exam software, and Palo Alto Networks Systems Engineer Professional - Hardware Firewall PSE-Strata-Pro-24 web-based practice test. TestInsides is aware that many PSE-Strata-Pro-24 exam applicants can't sit in front of a computer for many hours to study for the PSE-Strata-Pro-24 examination. If you are one of those Palo Alto Networks Systems Engineer Professional - Hardware Firewall PSE-Strata-Pro-24 exam candidates, don't worry because we have a portable file of Palo Alto Networks Palo Alto Networks Systems Engineer Professional - Hardware Firewall PDF Questions for you. Palo Alto Networks Systems Engineer Professional - Hardware Firewall PSE-Strata-Pro-24 PDF format works smoothly on all smart devices.

Palo Alto Networks PSE-Strata-Pro-24 Exam Syllabus Topics:

Topic	Details
Topic 1	• Deployment and Evaluation: This section of the exam measures the skills of Deployment Engineers and focuses on identifying the capabilities of Palo Alto Networks NGFWs. Candidates will evaluate features that protect against both known and unknown threats. They will also explain identity management from a deployment perspective and describe the proof of value (PoV) process, which includes assessing the effectiveness of NGFW solutions.
Topic 2	• Architecture and Planning: This section of the exam measures the skills of Network Architects and emphasizes understanding customer requirements and designing suitable deployment architectures. Candidates must explain Palo Alto Networks' platform networking capabilities in detail and evaluate their suitability for various environments. Handling aspects like system sizing and fine-tuning is also a critical skill assessed in this domain.

Topic 3	• Network Security Strategy and Best Practices: This section of the exam measures the skills of Security Strategy Specialists and highlights the importance of the Palo Alto Networks five-step Zero Trust methodology. Candidates must understand how to approach and apply the Zero Trust model effectively while emphasizing best practices to ensure robust network security.
Topic 4	• Business Value and Competitive Differentiators: This section of the exam measures the skills of Technical Business Value Analysts and focuses on identifying the value proposition of Palo Alto Networks Next-Generation Firewalls (NGFWs). Candidates will assess the technical business benefits of tools like Panorama and SCM. They will also recognize customer-relevant topics and align them with Palo Alto Networks' best solutions. Additionally, understanding Strata's unique differentiators is a key component of this domain.

PSE-Strata-Pro-24 Accurate Prep Material - PSE-Strata-Pro-24 Reliable Real Exam

Since One of the significant factors to judge whether one is competent or not is his or her PSE-Strata-Pro-24 certificates. So to get PSE-Strata-Pro-24 real exam and pass the PSE-Strata-Pro-24 exam is important. Generally speaking, certificates function as the fundamental requirement when a company needs to increase manpower in its start-up stage. In this respect, our PSE-Strata-Pro-24 practice materials can satisfy your demands if you are now in preparation for a certificate. We will be your best friend to help you achieve success!

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q31-Q36):

NEW QUESTION # 31
There are no Advanced Threat Prevention log events in a company's SIEM instance. However, the systems administrator has confirmed that the Advanced Threat Prevention subscription is licensed and that threat events are visible in the threat logs on the firewall.
Which action should the systems administrator take next?

- A. Have the SIEM vendor troubleshoot its software.
- B. Check with the SIEM vendor to verify that Advanced Threat Prevention logs are reaching the company's SIEM instance.
- C. Enable the company's Threat Prevention license.
- D. Ensure the Security policy rules that use Advanced Threat Prevention are set for log forwarding to the correct SIEM.

Answer: D

Explanation:
* Understanding the Problem:
* The issue is thatAdvanced Threat Prevention (ATP) logsare visible on the firewall but are not being ingested into the company's SIEM.
* This implies that the ATP subscription is working and generating logs on the firewall but the logs are not being forwarded properly to the SIEM.
* Action to Resolve:
* Log Forwarding Configuration:
* Verify that the Security policy rules configured to inspect traffic using Advanced Threat Prevention are set toforward logsto the SIEM instance.
* This is a common oversight. Even if the logs are generated locally, they will not be forwarded unless explicitly configured.
* Configuration steps to verify in the Palo Alto Networks firewall:
* Go toPolicies > Security Policiesand check the "Log Forwarding" profile applied.
* Ensure the "Log Forwarding" profile includes the correct settings to forwardThreat Logsto the SIEM.
* Go toDevice > Log Settingsand ensure the firewall is set to forward Threat logs to the desired Syslog or SIEM destination.
* Why Not the Other Options?
* A (Enable the Threat Prevention license):
* The problem does not relate to the license; the administrator already confirmed the license is active.

* B (Check with the SIEM vendor):
* While verifying SIEM functionality is important, the first step is to ensure the logs are being forwarded correctly from the firewall to the SIEM. This is under the systems administrator's control.
* C (Have the SIEM vendor troubleshoot):
* This step should only be takenafterconfirming the logs are forwarded properly from the firewall.
References from Palo Alto Networks Documentation:
* Log Forwarding and Security Policy Configuration
* Advanced Threat Prevention Configuration Guide

NEW QUESTION # 32
What is used to stop a DNS-based threat?

- A. DNS proxy
- B. Buffer overflow protection
- C. DNS tunneling
- D. DNS sinkholing

Answer: D

Explanation:
DNS-based threats, such as DNS tunneling, phishing, or malware command-and-control (C2) activities, are commonly used by attackers to exfiltrate data or establish malicious communications. Palo Alto Networks firewalls provide several mechanisms to address these threats, and the correct method is DNS sinkholing.
* Why "DNS sinkholing" (Correct Answer D)?DNS sinkholing redirects DNS queries for malicious domains to an internal or non-routable IP address, effectively preventing communication with malicious domains. When a user or endpoint tries to connect to a malicious domain, the sinkhole DNS entry ensures the traffic is blocked or routed to a controlled destination.
* DNS sinkholing is especially effective for blocking malware trying to contact its C2 server or preventing data exfiltration.
* Why not "DNS proxy" (Option A)?A DNS proxy is used to forward DNS queries from endpoints to an upstream DNS server. While it can be part of a network's DNS setup, it does not actively stop DNS- based threats.
* Why not "Buffer overflow protection" (Option B)?Buffer overflow protection is a method used to prevent memory-related attacks, such as exploiting software vulnerabilities. It is unrelated to DNS- based threat prevention.
* Why not "DNS tunneling" (Option C)?DNS tunneling is itself a type of DNS-based threat where attackers encode malicious traffic within DNS queries and responses. This option refers to the threat itself, not the method to stop it.
Reference: Palo Alto Networks DNS Security documentation confirms that DNS sinkholing is a key mechanism for stopping DNS-based threats.

NEW QUESTION # 33
When a customer needs to understand how Palo Alto Networks NGFWs lower the risk of exploitation by newly announced vulnerabilities known to be actively attacked, which solution and functionality delivers the most value?

- A. Advanced URL Filtering uses machine learning (ML) to learn which malicious URLs are being utilized by the attackers, then block the resulting traffic.
- B. Single Pass Architecture and parallel processing ensure traffic is efficiently scanned against any enabled Cloud-Delivered Security Services (CDSS) subscription.
- C. Advanced Threat Prevention's command injection and SQL injection functions use inline deep learning against zero-day threats.
- D. WildFire loads custom OS images to ensure that the sandboxing catches any activity that would affect the customer's environment.

Answer: C

Explanation:
The most effective way to reduce the risk of exploitation by newly announced vulnerabilities is through Advanced Threat Prevention (ATP). ATP uses inline deep learning to identify and block exploitation attempts, even for zero-day vulnerabilities, in real time.
* Why "Advanced Threat Prevention's command injection and SQL injection functions use inline deep learning against zero-day threats" (Correct Answer B)?Advanced Threat Prevention leverages deep learning models directly in the data path, which allows it to analyze traffic in real time and detect patterns of exploitation, including newly discovered vulnerabilities being actively exploited in the wild.
It specifically targets advanced tactics like:

* Command injection.
* SQL injection.
* Memory-based exploits.
* Protocol evasion techniques.
This functionality lowers the risk of exploitation by actively blocking attack attempts based on their behavior, even when a signature is not yet available. This approach makes ATP the most valuable solution for addressing new and actively exploited vulnerabilities.
* Why not "Advanced URL Filtering uses machine learning (ML) to learn which malicious URLs are being utilized by the attackers, then block the resulting traffic" (Option A)?While Advanced URL Filtering is highly effective at blocking access to malicious websites, it does not provide the inline analysis necessary to prevent direct exploitation of vulnerabilities. Exploitation often happens within the application or protocol layer, which Advanced URL Filtering does not inspect.
* Why not "Single Pass Architecture and parallel processing ensure traffic is efficiently scanned against any enabled Cloud-Delivered Security Services (CDSS) subscription" (Option C)?Single Pass Architecture improves performance by ensuring all enabled services (like Threat Prevention, URL Filtering, etc.) process traffic efficiently. However, it is not a feature that directly addresses vulnerability exploitation or zero-day attack detection.
* Why not "WildFire loads custom OS images to ensure that the sandboxing catches any activity that would affect the customer's environment" (Option D)?WildFire is a sandboxing solution designed to detect malicious files and executables. While it is useful for analyzing malware, it does not provide inline protection against exploitation of newly announced vulnerabilities, especially those targeting network protocols or applications.
Reference: Palo Alto Networks Advanced Threat Prevention specifically highlights its capability to detect and block zero-day exploits, leveraging inline deep learning and machine learning models. This makes it the optimal solution for protecting against new vulnerabilities being actively exploited.

NEW QUESTION # 34
Which initial action can a network security engineer take to prevent a malicious actor from using a file- sharing application for data exfiltration without impacting users who still need to use file-sharing applications?

- A. Use DNS Security to block all file-sharing applications and uploading abilities.
- B. Use DNS Security to limit access to file-sharing applications based on job functions.
- C. Use App-ID to block all file-sharing applications and uploading abilities.
- D. Use App-ID to limit access to file-sharing applications based on job functions.

Answer: D

Explanation:
To prevent malicious actors from abusing file-sharing applications for data exfiltration,App-IDprovides a granular approach to managing application traffic. Palo Alto Networks'App-IDis a technology that identifies applications traversing the network, regardless of port, protocol, encryption (SSL), or evasive tactics. By leveraging App-ID, security engineers can implement policies that restrict the use of specific applications or functionalities based on job functions, ensuring that only authorized users or groups can use file-sharing applications while blocking unauthorized or malicious usage.
Here's why the options are evaluated this way:
* Option A:DNS Security focuses on identifying and blocking malicious domains. While it plays a critical role in preventing certain attacks (like command-and-control traffic), it is not effective for managing application usage. Hence, this is not the best approach.
* Option B (Correct):App-ID provides the ability to identify file-sharing applications (such as Dropbox, Google Drive, or OneDrive) and enforce policies to restrict their use. For example, you can create a security rule allowing file-sharing apps only for specific job functions, such as HR or marketing, while denying them for other users. This targeted approach ensures legitimate business needs are not disrupted, which aligns with the requirement of not impacting valid users.
* Option C:Blocking all file-sharing applications outright using DNS Security is a broad measure that will indiscriminately impact legitimate users. This does not meet the requirement of allowing specific users to continue using file-sharing applications.
* Option D:While App-ID can block file-sharing applications outright, doing so will prevent legitimate usage and is not aligned with the requirement to allow usage based on job functions.
How to Implement the Solution (Using App-ID):
* Identify the relevant file-sharing applications using App-ID in Palo Alto Networks' predefined application database.
* Create security policies that allow these applications only for users or groups defined in your directory (e.g., Active Directory).
* Use custom App-ID filters or explicit rules to control specific functionalities of file-sharing applications, such as uploads or downloads.
* Monitor traffic to ensure that only authorized users are accessing the applications and that no malicious activity is occurring.
References:
* Palo Alto Networks Admin Guide: Application Identification and Usage Policies.
* Best Practices for App-ID Configuration: https://docs.paloaltonetworks.com

NEW QUESTION # 35
In addition to Advanced DNS Security, which three Cloud-Delivered Security Services (CDSS) subscriptions utilize inline machine learning (ML)? (Choose three)

- A. Advanced Threat Prevention
- B. IoT Security
- C. Enterprise DLP
- D. Advanced WildFire
- E. Advanced URL Filtering

Answer: A,C,E

Explanation:
To answer this question, let's analyze each Cloud-Delivered Security Service (CDSS) subscription and its role in inline machine learning (ML). Palo Alto Networks leverages inline ML capabilities across several of its subscriptions to provide real-time protection against advanced threats and reduce the need for manual intervention.
A: Enterprise DLP (Data Loss Prevention)
Enterprise DLP is a Cloud-Delivered Security Service that prevents sensitive data from being exposed. Inline machine learning is utilized to accurately identify and classify sensitive information in real-time, even when traditional data patterns or signatures fail to detect them. This service integrates seamlessly with Palo Alto firewalls to mitigate data exfiltration risks by understanding content as it passes through the firewall.
B: Advanced URL Filtering
Advanced URL Filtering uses inline machine learning to block malicious URLs in real-time. Unlikelegacy URL filtering solutions, which rely on static databases, Palo Alto Networks' Advanced URL Filtering leverages ML to identify and stop new malicious URLs that have not yet been categorized in static databases.
This proactive approach ensures that organizations are protected against emerging threats like phishing and malware-hosting websites.
C: Advanced WildFire
Advanced WildFire is a cloud-based sandboxing solution designed to detect and prevent zero-day malware.
While Advanced WildFire is a critical part of Palo Alto Networks' security offerings, it primarily uses static and dynamic analysis rather than inline machine learning. The ML-based analysis in Advanced WildFire happens after a file is sent to the cloud for processing, rather than inline, so it does not qualify under this question's scope.
D: Advanced Threat Prevention
Advanced Threat Prevention (ATP) uses inline machine learning to analyze traffic in real-time and block sophisticated threats such as unknown command-and-control (C2) traffic. This service replaces the traditional Intrusion Prevention System (IPS) approach by actively analyzing network traffic and blocking malicious payloads inline. The inline ML capabilities ensure ATP can detect and block threats that rely on obfuscation and evasion techniques.
E: IoT Security
IoT Security is focused on discovering and managing IoT devices connected to the network. While this service uses machine learning for device behavior profiling and anomaly detection, it does not leverage inline machine learning for real-time traffic inspection. Instead, it operates at a more general level by providing visibility and identifying device risks.
Key Takeaways:
* Enterprise DLP, Advanced URL Filtering, and Advanced Threat Prevention all rely on inline machine learning to provide real-time protection.
* Advanced WildFire uses ML but not inline; its analysis is performed in the cloud.
* IoT Security applies ML for device management rather than inline threat detection.

NEW QUESTION # 36
.....

Hardware Firewall Reliable Dumps Pass Guaranteed □ Simply search for （ PSE-Strata-Pro-24 ） for free download on ✔ www.troytecdumps.com □✔□ □New PSE-Strata-Pro-24 Braindumps Sheet

- Upgrade PSE-Strata-Pro-24 Dumps □ Latest Braindumps PSE-Strata-Pro-24 Ppt □ PSE-Strata-Pro-24 Study Tool □ □ Go to website { www.pdfvce.com } open and search for ➥ PSE-Strata-Pro-24 □ to download for free □PSE-Strata-Pro-24 Test Torrent
- Simulation PSE-Strata-Pro-24 Questions □ Simulation PSE-Strata-Pro-24 Questions ↖ Trustworthy PSE-Strata-Pro-24 Source □ Immediately open ➡ www.torrentvce.com □□□ and search for 《 PSE-Strata-Pro-24 》 to obtain a free download □PSE-Strata-Pro-24 Official Practice Test
- Valid PSE-Strata-Pro-24 Test Discount □ Valid PSE-Strata-Pro-24 Test Discount □ PSE-Strata-Pro-24 Cost Effective Dumps □ Search for 【 PSE-Strata-Pro-24 】 and download it for free on 「 www.pdfvce.com 」 website □ □New PSE-Strata-Pro-24 Braindumps Sheet
- Experience the real Palo Alto Networks exam environment with our web-based PSE-Strata-Pro-24 practice test □ Download ➡ PSE-Strata-Pro-24 □□□ for free by simply searching on { www.validtorrent.com } □Test PSE-Strata-Pro-24 Questions
- PSE-Strata-Pro-24 Reliable Dumps - Realistic Palo Alto Networks Palo Alto Networks Systems Engineer Professional - Hardware Firewall Reliable Dumps Pass Guaranteed □ Search on ➽ www.pdfvce.com □ for " PSE-Strata-Pro-24 " to obtain exam materials for free download □PSE-Strata-Pro-24 Study Tool
- Free PDF Quiz Pass-Sure Palo Alto Networks - PSE-Strata-Pro-24 Reliable Dumps □ Download ➠ PSE-Strata-Pro-24 □ for free by simply searching on □ www.prep4away.com □ □PSE-Strata-Pro-24 Valid Test Question
- PSE-Strata-Pro-24 Official Practice Test □ PSE-Strata-Pro-24 Cost Effective Dumps □ PSE-Strata-Pro-24 Valid Exam Answers □ Open " www.pdfvce.com " and search for [PSE-Strata-Pro-24] to download exam materials for free □Interactive PSE-Strata-Pro-24 Questions
- PSE-Strata-Pro-24 Exam Guide: Palo Alto Networks Systems Engineer Professional - Hardware Firewall - PSE-Strata-Pro-24 Exam Collection □ Open ✔ www.testkingpass.com □✔□ and search for " PSE-Strata-Pro-24 " to download exam materials for free □Latest Braindumps PSE-Strata-Pro-24 Ppt
- Pass Guaranteed Trustable Palo Alto Networks - PSE-Strata-Pro-24 - Palo Alto Networks Systems Engineer Professional - Hardware Firewall Reliable Dumps □ Open [www.pdfvce.com] enter 《 PSE-Strata-Pro-24 》 and obtain a free download □PSE-Strata-Pro-24 New Braindumps Sheet
- PSE-Strata-Pro-24 New Braindumps Sheet □ PSE-Strata-Pro-24 Valid Test Question □ Real PSE-Strata-Pro-24 Exam Questions □ Search for ➠ PSE-Strata-Pro-24 □ and download it for free on ➠ www.troytecdumps.com □ website □PSE-Strata-Pro-24 Test Assessment
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, 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.divephotoguide.com, 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, 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, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of TestInsides PSE-Strata-Pro-24 dumps from Cloud Storage: https://drive.google.com/open?id=1BzEYIZcsBn602JB9oZz5cSH1FOHPIYv8