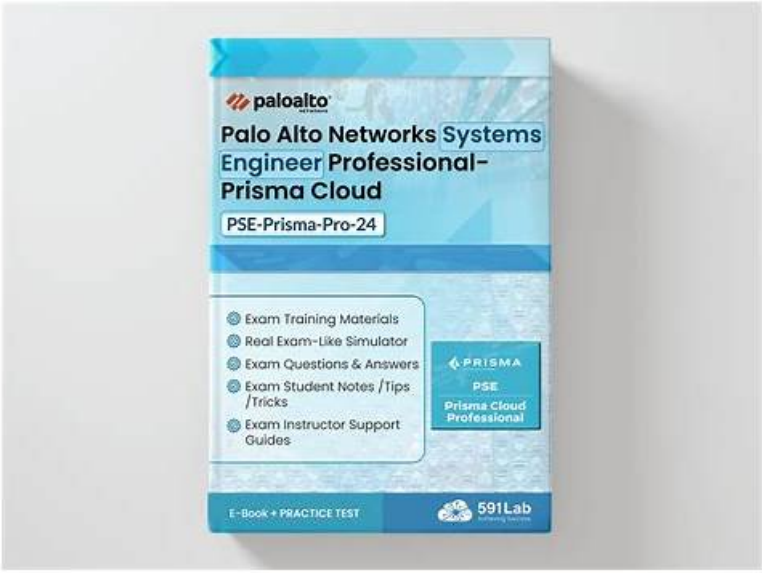
Palo Alto Networks PSE-Strata-Pro-24 Reliable Test Cost | PSE-Strata-Pro-24 Free Updates



BONUS!!! Download part of GetValidTest PSE-Strata-Pro-24 dumps for free: https://drive.google.com/open?id=13j9wRWOm519OLb83daonkinJ3F-ge-fZ

we believe that all students who have purchased PSE-Strata-Pro-24 practice materials will be able to successfully pass the professional PSE-Strata-Pro-24 qualification exam as long as they follow the content provided by our PSE-Strata-Pro-24 study materials, study it on a daily basis, and conduct regular self-examination through mock exams. Of course, before you buy, our PSE-Strata-Pro-24 Study Materials offer you a free trial service, as long as you log on our website, you can download our trial questions bank for free. I believe that after you try PSE-Strata-Pro-24 test engine, you will love them.

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

Topic	Details
Topic 1	• 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 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	• 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 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.

>> Palo Alto Networks PSE-Strata-Pro-24 Reliable Test Cost <<

PSE-Strata-Pro-24 Free Updates - PSE-Strata-Pro-24 Testking Learning Materials

The Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) practice exam software in desktop and web-based versions has a lot of premium features. One of which is the customization of Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) practice exams. The PSE-Strata-Pro-24 Practice Tests are specially made for the customers so that they can practice unlimited times and improve day by day and pass Palo Alto Networks PSE-Strata-Pro-24 certification exam with good grades.

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q23-Q28):

NEW QUESTION # 23
While a quote is being finalized for a customer that is purchasing multiple PA-5400 series firewalls, the customer specifies the need for protection against zero-day malware attacks.
Which Cloud-Delivered Security Services (CDSS) subscription add-on license should be included in the quote?

- A. App-ID
- B. Advanced Threat Prevention
- C. Advanced WildFire
- D. AI Access Security

Answer: C

Explanation:
Zero-day malware attacks are sophisticated threats that exploit previously unknown vulnerabilities or malware signatures. To provide protection against such attacks, the appropriate Cloud-Delivered Security Service subscription must be included.
* Why "Advanced WildFire" (Correct Answer C)?Advanced WildFire is Palo Alto Networks' sandboxing solution that identifies and prevents zero-day malware. It uses machine learning, dynamic analysis, and static analysis to detect unknown malware in real time.
* Files and executables are analyzed in the cloud-based sandbox, and protections are shared globally within minutes.
* Advanced WildFire specifically addresses zero-day threats by dynamically analyzing suspicious files and generating new signatures.
* Why not "AI Access Security" (Option A)?AI Access Security is designed to secure SaaS applications by monitoring and enforcing data protection and compliance. While useful for SaaS security, it does not focus on detecting or preventing zero-day malware.
* Why not "Advanced Threat Prevention" (Option B)?Advanced Threat Prevention (ATP) focuses on detecting zero-day exploits (e.g., SQL injection, buffer overflows) using inline deep learning but is not specifically designed to analyze and prevent zero-day malware. ATP complements Advanced WildFire, but WildFire is the primary solution for malware detection.
* Why not "App-ID" (Option D)?App-ID identifies and controls applications on the network. While it improves visibility and security posture, it does not address zero-day malware detection or prevention.

NEW QUESTION # 24
A prospective customer is concerned about stopping data exfiltration, data infiltration, and command-and- control (C2) activities over port 53.
Which subscription(s) should the systems engineer recommend?

- A. Advanced Threat Prevention and Advanced URL Filtering
- B. DNS Security
- C. App-ID and Data Loss Prevention
- D. Threat Prevention

Answer: B

Explanation:
* DNS Security (Answer C):
* DNS Securityis the appropriate subscription for addressingthreats over port 53.
* DNS tunneling is a common method used fordata exfiltration, infiltration, and C2 activities, as it allows malicious traffic to be hidden within legitimate DNS queries.
* The DNS Security service appliesmachine learning modelsto analyze DNSqueries in real-time, block malicious domains, and prevent tunneling activities.
* It integrates seamlessly with the NGFW, ensuring advanced protection against DNS-based threats without requiring additional infrastructure.
* Why Not Threat Prevention (Answer A):
* Threat Prevention is critical for blocking malware, exploits, and vulnerabilities, but it does not specifically addressDNS-based tunnelingor C2 activities over port 53.
* Why Not App-ID and Data Loss Prevention (Answer B):
* While App-ID can identify applications, and Data Loss Prevention (DLP) helps prevent sensitive data leakage, neither focuses on blockingDNS tunnelingor malicious activity over port 53.
* Why Not Advanced Threat Prevention and Advanced URL Filtering (Answer D):
* Advanced Threat Prevention and URL Filtering are excellent for broader web and network threats, but DNS tunneling specifically requires theDNS Security subscription, which specializes in DNS-layer threats.
References from Palo Alto Networks Documentation:
* DNS Security Subscription Overview

NEW QUESTION # 25
What does Policy Optimizer allow a systems engineer to do for an NGFW?

- A. Act as a migration tool to import policies from third-party vendors
- B. Identify Security policy rules with unused applications
- C. Recommend best practices on new policy creation
- D. Show unused licenses for Cloud-Delivered Security Services (CDSS) subscriptions and firewalls

Answer: B

Explanation:
Policy Optimizer is a feature designed to help administrators improve the efficiency and effectiveness of security policies on Palo Alto Networks Next-Generation Firewalls (NGFWs). It focuses on identifying unused or overly permissive policies to streamline and optimize the configuration.
* Why "Identify Security policy rules with unused applications" (Correct Answer C)?Policy Optimizer provides visibility into existing security policies and identifies rules that have unused or outdated applications. For example:
* It can detect if a rule allows applications that are no longer in use.
* It can identify rules with excessive permissions, enabling administrators to refine them for better security and performance.By addressing these issues, Policy Optimizer helps reduce the attack surface and improves the overall manageability of the firewall.
* Why not "Recommend best practices on new policy creation" (Option A)?Policy Optimizer focuses on optimizing existing policies, not creating new ones. While best practices can be applied during policy refinement, recommending new policy creation is not its purpose.
* Why not "Show unused licenses for Cloud-Delivered Security Services (CDSS) subscriptions and firewalls" (Option B)?Policy Optimizer is not related to license management or tracking. Identifying unused licenses is outside the scope of its functionality.
* Why not "Act as a migration tool to import policies from third-party vendors" (Option D)?Policy Optimizer does not function as a migration tool. While Palo Alto Networks offers tools for third-party firewall migration, this is separate from the Policy Optimizer feature.
Reference: The Palo Alto Networks Policy Optimizer documentation highlights its primary function of identifying unused or overly broad policy rules to optimize firewall configurations.

NEW QUESTION # 26
A systems engineer should create a profile that blocks which category to protect a customer from ransomware URLs by using Advanced URL Filtering?

- A. Ransomware
- B. Scanning Activity
- C. Command and Control

- D. High Risk

Answer: A

Explanation:
When configuring Advanced URL Filtering on a Palo Alto Networks firewall, the "Ransomware" category should be explicitly blocked to protect customers from URLs associated with ransomware activities.
Ransomware URLs typically host malicious code or scripts designed to encrypt user data and demand a ransom. By blocking the "Ransomware" category, systems engineers can proactively prevent users from accessing such URLs.
* Why "Ransomware" (Correct Answer A)?The "Ransomware" category is specifically curated by Palo Alto Networks to include URLs known to deliver ransomware or support ransomware operations.
Blocking this category ensures that any URL categorized as part of this list will be inaccessible to end- users, significantly reducing the risk of ransomware attacks.
* Why not "High Risk" (Option B)?While the "High Risk" category includes potentially malicious sites, it is broader and less targeted. It may not always block ransomware-specific URLs. "High Risk" includes a range of websites that are flagged based on factors like bad reputation or hosting malicious content in general. It is less focused than the "Ransomware" category.
* Why not "Scanning Activity" (Option C)?The "Scanning Activity" category focuses on URLs used in vulnerability scans, automated probing, or reconnaissance by attackers. Although such activity could be a precursor to ransomware attacks, it does not directly block ransomware URLs.
* Why not "Command and Control" (Option D)?The "Command and Control" category is designed to block URLs used by malware or compromised systems to communicate with their operators. While some ransomware may utilize command-and-control (C2) servers, blocking C2 URLs alone does not directly target ransomware URLs themselves.
By using the Advanced URL Filtering profile and blocking the "Ransomware" category, the firewall applies targeted controls to mitigate ransomware-specific threats.
Reference: Palo Alto Networks documentation for Advanced URL Filtering confirms that blocking the "Ransomware" category is a recommended best practice for preventing ransomware threats.

NEW QUESTION # 27
A security engineer has been tasked with protecting a company's on-premises web servers but is not authorized to purchase a web application firewall (WAF).
Which Palo Alto Networks solution will protect the company from SQL injection zero-day, command injection zero-day, Cross-Site Scripting (XSS) attacks, and IIS exploits?

- A. Advanced WildFire and PAN-OS 10.0 (and higher)
- B. Threat Prevention, Advanced URL Filtering, and PAN-OS 10.2 (and higher)
- C. Threat Prevention and PAN-OS 11.x
- D. Advanced Threat Prevention and PAN-OS 11.x

Answer: D

Explanation:
Protecting web servers from advanced threats like SQL injection, command injection, XSS attacks, and IIS exploits requires a solution capable of deep packet inspection, behavioral analysis, and inline prevention of zero-day attacks. The most effective solution here is Advanced Threat Prevention (ATP) combined with PAN-OS 11.x.
* Why "Advanced Threat Prevention and PAN-OS 11.x" (Correct Answer B)?Advanced Threat Prevention (ATP) enhances traditional threat prevention by using inline deep learning models to detect and block advanced zero-day threats, including SQL injection, command injection, and XSS attacks. With PAN-OS 11.x, ATP extends its detection capabilities to detect unknown exploits without relying on signature-based methods. This functionality is critical for protecting web servers in scenarios where a dedicated WAF is unavailable.
ATP provides the following benefits:
* Inline prevention of zero-day threats using deep learning models.
* Real-time detection of attacks like SQL injection and XSS.
* Enhanced protection for web server platforms like IIS.
* Full integration with the Palo Alto Networks Next-Generation Firewall (NGFW).
* Why not "Threat Prevention and PAN-OS 11.x" (Option A)?Threat Prevention relies primarily on signature-based detection for known threats. While it provides basic protection, it lacks the capability to block zero-day attacks using advanced methods like inline deep learning. For zero-day SQL injection and XSS attacks, Threat Prevention alone is insufficient.
* Why not "Threat Prevention, Advanced URL Filtering, and PAN-OS 10.2 (and higher)" (Option C)?While this combination includes Advanced URL Filtering (useful for blocking malicious URLs associated with exploits), it still relies on Threat Prevention, which is signature-based. This combination does not provide the zero-day protection needed for advanced injection attacks or XSS

vulnerabilities.
* Why not "Advanced WildFire and PAN-OS 10.0 (and higher)" (Option D)?Advanced WildFire is focused on analyzing files and executables in a sandbox environment to identify malware. While it is excellent for identifying malware, it is not designed to provide inline prevention for web-based injection attacks or XSS exploits targeting web servers.
Reference: The Palo Alto Networks Advanced Threat Prevention documentation highlights its ability to block zero-day injection attacks and web-based exploits by leveraging inline machine learning and behavioral analysis. This makes it the ideal solution for the described scenario.

NEW QUESTION # 28
......

Do you feel aimless and helpless when the PSE-Strata-Pro-24 exam is coming soon? If your answer is absolutely yes, then we would like to suggest you to try our PSE-Strata-Pro-24 training materials, which are high quality and efficiency test tools. Your success is 100% ensured to pass the PSE-Strata-Pro-24 Exam and acquire the dreaming certification which will enable you to reach for more opportunities to higher incomes or better enterprises.

PSE-Strata-Pro-24 Free Updates: https://www.getvalidtest.com/PSE-Strata-Pro-24-exam.html

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, Disposable vapes

P.S. Free & New PSE-Strata-Pro-24 dumps are available on Google Drive shared by GetValidTest: https://drive.google.com/open?id=13j9wRWOm519OLb83daonkinJ3F-ge-fZ