2026 PSE-Strata-Pro-24: Palo Alto Networks Systems Engineer Professional - Hardware Firewall–Reliable Passguide

Paloalto Networks PSE-Strata-Pro-24 Exam

Palo Alto Networks Systems Engineer Professional - Hardware Firewall

https://www.passquestion.com/pse-strata-pro-24.html

Save **35% OFF** on ALL Exams

Coupon: 2025

35% OFF on All, Including PSE-Strata-Pro-24 Questions and Answers

Pass **Paloalto Networks PSE-Strata-Pro-24** Exam with PassQuestion PSE-Strata-Pro-24 questions and answers in the first attempt.

https://www.passquestion.com/

2026 Latest It-Tests PSE-Strata-Pro-24 PDF Dumps and PSE-Strata-Pro-24 Exam Engine Free Share: https://drive.google.com/open?id=1wuBOecL707vkQSIinvy6CJ4bky3XZawj

Once the user has used our PSE-Strata-Pro-24 learning material for a mock exercise, the product's system automatically remembers and analyzes all the user's actual operations. The user must complete the test within the time specified by the simulation system, and there is a timer on the right side of the screen, as long as the user begins the practice of PSE-Strata-Pro-24 Learning Materials, the timer will run automatic and start counting.

Some practice materials keep droning on the useless points of knowledge. In contrast, being venerated for high quality and accuracy rate, our PSE-Strata-Pro-24 training quiz received high reputation for their efficiency and accuracy rate originating from your interests, and the whole review process may cushier than you have imagined before. Numerous of our loyal customers wrote to us to praise that the PSE-Strata-Pro-24 Exam Questions are the same with the real exam questions and they passed PSE-Strata-Pro-24 exam with ease.

>> PSE-Strata-Pro-24 Passguide <<

PSE-Strata-Pro-24 Free Study Material, PSE-Strata-Pro-24 Trustworthy

Practice

Our PSE-Strata-Pro-24 quiz torrent can provide you with a free trial version, thus helping you have a deeper understanding about our PSE-Strata-Pro-24 test prep and estimating whether this kind of study material is suitable to you or not before purchasing. With the help of our trial version, you will have a closer understanding about our PSE-Strata-Pro-24 exam torrent from different aspects, ranging from choice of three different versions available on our test platform to our after-sales service. Otherwise you may still be skeptical and unintelligible about our PSE-Strata-Pro-24 Test Prep. So as you see, we are the corporation with ethical code and willing to build mutual trust between our customers.

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

Topic	Details
Topic 1	• 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 2	• 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 3	• 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.
Topic 4	• 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.

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q61-Q66):

NEW QUESTION # 61
A customer sees unusually high DNS traffic to an unfamiliar IP address. Which Palo Alto Networks Cloud-Delivered Security Services (CDSS) subscription should be enabled to further inspect this traffic?

- A. Advanced DNS Security
- B. Advanced URL Filtering
- C. Advanced Threat Prevention
- D. Advanced WildFire

Answer: A

Explanation:
The appropriate CDSS subscription to inspect and mitigate suspicious DNS traffic isAdvanced DNS Security
. Here's why:
* Advanced DNS Securityprotects against DNS-based threats, including domain generation algorithms (DGA), DNS tunneling (often used for data exfiltration), and malicious domains used in attacks. It leverages machine learning to detect and block DNS traffic associated with command-and-control servers or other malicious activities. In this case, unusually high DNS traffic to an unfamiliar IP address is likely indicative of a DNS-based attack or malware activity, making this the most suitable service.
* Option A:Advanced Threat Prevention (ATP) focuses on identifying and blocking sophisticated threats in network traffic, such as

exploits and evasive malware. While it complements DNS Security, it does not specialize in analyzing DNS-specific traffic patterns.
* Option B:Advanced WildFire focuses on detecting and preventing file-based threats, such as malware delivered via email attachments or web downloads. It does not provide specific protection for DNS- related anomalies.
* Option C:Advanced URL Filtering is designed to prevent access to malicious or inappropriate websites based on their URLs. While DNS may be indirectly involved in resolving malicious websites, this service does not directly inspect DNS traffic patterns for threats.
* Option D (Correct):Advanced DNS Security specifically addresses DNS-based threats. By enabling this service, the customer can detect and block DNS queries to malicious domains and investigate anomalous DNS behavior like the high traffic observed in this scenario.
How to Enable Advanced DNS Security:
* Ensure the firewall has a valid Advanced DNS Security license.
* Navigate toObjects > Security Profiles > Anti-Spyware.
* Enable DNS Security under the "DNS Signatures" section.
* Apply the Anti-Spyware profile to the relevant Security Policy to enforce DNS Security.
References:
* Palo Alto Networks Advanced DNS Security Overview: https://www.paloaltonetworks.com/dns- security
* Best Practices for DNS Security Configuration.

NEW QUESTION # 62

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

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.
Reference: Palo Alto Networks Advanced WildFire documentation confirms its role in detecting and preventing zero-day malware through advanced analysis techniques.

NEW QUESTION # 63

A customer asks a systems engineer (SE) how Palo Alto Networks can claim it does not lose throughput performance as more Cloud-Delivered Security Services (CDSS) subscriptions are enabled on the firewall.
Which two concepts should the SE explain to address the customer's concern? (Choose two.)

- A. Parallel Processing
- B. Management Data Plane Separation
- C. Single Pass Architecture

- D. Advanced Routing Engine

Answer: A,C

Explanation:
The customer's question focuses on how Palo Alto Networks Strata Hardware Firewalls maintain throughput performance as more Cloud-Delivered Security Services (CDSS) subscriptions-such as Threat Prevention, URL Filtering, WildFire, DNS Security, and others-are enabled. Unlike traditional firewalls where enabling additional security features often degrades performance, Palo Alto Networks leverages its unique architecture to minimize this impact. The systems engineer (SE) should explain two key concepts-Parallel Processing and Single Pass Architecture-which are foundational to the firewall's ability to sustain throughput. Below is a detailed explanation, verified against Palo Alto Networks documentation.
Step 1: Understanding Cloud-Delivered Security Services (CDSS) and Performance Concerns CDSS subscriptions enhance the Strata Hardware Firewall's capabilities by integrating cloud-based threat intelligence and advanced security features into PAN-OS. Examples include:
* Threat Prevention: Blocks exploits, malware, and command-and-control traffic.
* WildFire: Analyzes unknown files in the cloud for malware detection.
* URL Filtering: Categorizes and controls web traffic.
Traditionally, enabling such services on other firewalls increases processing overhead, as each feature requires separate packet scans or additional hardware resources, leading to latency and throughput loss. Palo Alto Networks claims consistent performance due to its innovative design, rooted in the Single Pass Parallel Processing (SP3) architecture.
Reference: Palo Alto Networks Cloud-Delivered Security Services Overview
"CDSS subscriptions integrate with NGFWs to deliver prevention-oriented security without compromising performance, leveraging the SP3 architecture." Step 2: Explaining the Relevant Concepts The SE should focus on A. Parallel Processing and C. Single Pass Architecture, as these directly address how throughput is maintained when CDSS subscriptions are enabled.
Concept A: Parallel Processing
Definition: Parallel Processing refers to the hardware architecture in Palo Alto Networks NGFWs, where specialized processors handle distinct functions (e.g., networking, security, decryption) simultaneously. This is achieved through a separation of duties across dedicated hardware components, such as the Network Processor, Security Processor, and Signature Matching Processor, all working in parallel.
How It Addresses the Concern: When CDSS subscriptions are enabled, tasks like threat signature matching (Threat Prevention), URL categorization (URL Filtering), or file analysis forwarding (WildFire) are offloaded to specific processors. These operate concurrently rather than sequentially, preventing bottlenecks. The parallel execution ensures that adding more security services doesn't linearly increase processing time or reduce throughput.
Technical Detail:
Network Processor: Handles routing, NAT, and flow lookup.
Security Processor: Manages encryption/decryption and policy enforcement.
Signature Matching Processor: Performs content inspection for threats and CDSS features.
High-speed buses (e.g., 1Gbps in high-end models) connect these processors, enabling rapid data transfer.
Outcome: Throughput remains high because the workload is distributed across parallel hardware resources, not stacked on a single CPU.
Reference: PAN-OS Administrator's Guide (11.1) - Hardware Architecture
"Parallel Processing hardware ensures that function-specific tasks are executed concurrently, maintaining performance as security services scale." Concept C: Single Pass Architecture Definition: Single Pass Architecture is the software approach in PAN-OS where a packet is processed once, with all necessary functions-networking, policy lookup, App-ID, User-ID, decryption, and content inspection (including CDSS features)-performed in a single pass. This contrasts with multi-pass architectures, where packets are scanned repeatedly for each enabled feature.
How It Addresses the Concern: When CDSS subscriptions are activated, their inspection tasks (e.g., threat signatures, URL checks) are integrated into the single-pass process. The packet isn't reprocessed for each service; instead, a stream-based, uniform signature-matching engine applies all relevant checks in one go.
This minimizes latency and preserves throughput, as the overhead of additional services is marginal.
Technical Detail:
A packet enters the firewall and is classified by App-ID.
Decryption (if needed) occurs, exposing content.
A single Content-ID engine scans the stream for threats, URLs, and other CDSS-related patterns simultaneously.
Policy enforcement and logging occur without additional passes.
Outcome: Enabling more CDSS subscriptions adds rules to the existing scan, not new processing cycles, ensuring consistent performance.
Reference: Palo Alto Networks Single Pass Architecture Whitepaper
"Single Pass software performs all security functions in one pass, eliminating redundant processing and maintaining high throughput even with multiple services enabled." Step 3: Evaluating the Other Options To confirm A and C are correct, let's examine why B and D don't directly address the throughput concern:

B). Advanced Routing Engine:
Analysis: The Advanced Routing Engine in PAN-OS enhances routing capabilities (e.g., BGP, OSPF) and supports features like path monitoring. While important for network performance, it doesn't directly influence the processing of CDSS subscriptions, which occur at the security and content inspection layers, not the routing layer.
Conclusion: Not relevant to the question.
Reference: PAN-OS Administrator's Guide (11.1) - Routing Overview - "The Advanced Routing Engine optimizes network paths but is separate from security processing." D). Management Data Plane Separation:
Analysis: This refers to the separation of the control plane (management tasks like configuration and logging) and data plane (packet processing). It ensures management tasks don't impact traffic processing but doesn't directly address how CDSS subscriptions affect throughput within the data plane itself.
Conclusion: Indirectly supportive but not a primary explanation.
Reference: PAN-OS Administrator's Guide (11.1) - Hardware Architecture - "Control and data plane separation prevents management load from affecting throughput." Step 4: Tying It Together for the Customer The SE should explain:
Parallel Processing: "Our firewalls use dedicated hardware processors working in parallel for networking, security, and threat inspection. When you enable more CDSS subscriptions, the workload is spread across these processors, so throughput doesn't drop." Single Pass Architecture: "Our software processes each packet once, applying all security checks-including CDSS features-in a single scan. This avoids the performance hit you'd see with other firewalls that reprocess packets for each new service." This dual approach-hardware parallelism and software efficiency-ensures the firewall scales security without sacrificing speed.

NEW QUESTION # 64
Which three tools can a prospective customer use to evaluate Palo Alto Networks products to assess where they will fit in the existing architecture? (Choose three)

- A. Ultimate Test Drive
- B. Policy Optimizer
- C. Security Lifecycle Review (SLR)
- D. Expedition
- E. Proof of Concept (POC)

Answer: A,C,E

Explanation:
When evaluating Palo Alto Networks products, prospective customers need tools that can help them assess compatibility, performance, and value within their existing architecture. The following tools are the most relevant:
* Why "Proof of Concept (POC)" (Correct Answer A)?A Proof of Concept is a hands-on evaluation that allows the customer to deploy and test Palo Alto Networks products directly within their environment. This enables them to assess real-world performance, compatibility, and operational impact.
* Why "Security Lifecycle Review (SLR)" (Correct Answer C)?An SLR provides a detailed report of a customer's network security posture based on data collected during a short evaluation period. It highlights risks, vulnerabilities, and active threats in the customer's network, demonstrating how Palo Alto Networks solutions can address those risks. SLR is a powerful tool for justifying the value of a product in the customer's architecture.
* Why "Ultimate Test Drive" (Correct Answer D)?The Ultimate Test Drive is a guided hands-on workshop provided by Palo Alto Networks that allows prospective customers to explore product features and capabilities in a controlled environment. It is ideal for customers who want to evaluate products without deploying them in their production network.
* Why not "Policy Optimizer" (Option B)?Policy Optimizer is used after a product has been deployed to refine security policies by identifying unused or overly permissive rules. It is not designed for pre- deployment evaluations.
* Why not "Expedition" (Option E)?Expedition is a migration tool that assists with the conversion of configurations from third-party firewalls or existing Palo Alto Networks firewalls. It is not a tool for evaluating the suitability of products in the customer's architecture.

NEW QUESTION # 65
Which three descriptions apply to a perimeter firewall? (Choose three.)

- A. Network layer protection for the outer edge of a network
- B. Securing east-west traffic in a virtualized data center with flexible resource allocation
- C. Power utilization less than 500 watts sustained
- D. Primarily securing north-south traffic entering and leaving the network
- E. Guarding against external attacks

Answer: A,D,E

Explanation:
Aperimeter firewallis traditionally deployed at the boundary of a network to protect it from external threats.
It provides a variety of protections, including blocking unauthorized access, inspecting traffic flows, and safeguarding sensitive resources. Here is how the options apply:
* Option A (Correct):Perimeter firewalls providenetwork layer protectionby filtering and inspecting traffic entering or leaving the network at the outer edge. This is one of their primary roles.
* Option B:Power utilization is not a functional or architectural aspect of a firewall and is irrelevant when describing the purpose of a perimeter firewall.
* Option C:Securing east-west traffic is more aligned withdata center firewalls, whichmonitor lateral (east-west) movement of traffic within a virtualized or segmented environment. A perimeter firewall focuses on north-south traffic instead.
* Option D (Correct):A perimeter firewall primarily securesnorth-south traffic, which refers to traffic entering and leaving the network. It ensures that inbound and outbound traffic adheres to security policies.
* Option E (Correct):Perimeter firewalls play a critical role inguarding against external attacks, such as DDoS attacks, malicious IP traffic, and other unauthorized access attempts.
References:
* Palo Alto Networks Firewall Deployment Use Cases: https://docs.paloaltonetworks.com
* Security Reference Architecture for North-South Traffic Control.

NEW QUESTION # 66
......

While PSE-Strata-Pro-24 exam preparing for the Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) exam, candidates have to pay extra money when Palo Alto Networks introduces new changes. With It-Tests you can save money in this scenario as up to 365 days of free updates are available. You can also download a free demo to understand everything about It-Tests PSE-Strata-Pro-24 Exam Material before buying.

PSE-Strata-Pro-24 Free Study Material: https://www.it-tests.com/PSE-Strata-Pro-24.html