

PSE-Strata-Pro-24 Latest Learning Materials, Valid PSE-Strata-Pro-24 Test Online



P.S. Free & New PSE-Strata-Pro-24 dumps are available on Google Drive shared by PassSureExam:
<https://drive.google.com/open?id=1X7UgZBqfZ-fBV9A1KuFJAhtYL1mPFy3x>

Do you want to find a job that really fulfills your ambitions? That's because you haven't found an opportunity to improve your ability to lay a solid foundation for a good career. Our PSE-Strata-Pro-24 learning materials are carefully compiled by industry experts based on the examination questions and industry trends in the past few years. The knowledge points are comprehensive and focused. You don't have to worry about our learning from PSE-Strata-Pro-24 Exam Question. We assure you that our PSE-Strata-Pro-24 learning materials are easy to understand and use the fewest questions to convey the most important information.

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

Topic	Details
Topic 1	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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 3	<ul style="list-style-type: none">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	<ul style="list-style-type: none"> • 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 Latest Learning Materials <<

Valid PSE-Strata-Pro-24 Test Online, Training PSE-Strata-Pro-24 Pdf

The Palo Alto Networks PSE-Strata-Pro-24 certification is one of the top-rated career advancement certifications in the market. This Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) certification exam has been inspiring candidates since its beginning. Over this long time period, thousands of PSE-Strata-Pro-24 exam candidates have passed their Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) certification exam and now they are doing jobs in the world's top brands. The PassSureExam PSE-Strata-Pro-24 Dumps will provide you with everything that you need to learn, prepare and pass the challenging Network Security Specialist PSE-Strata-Pro-24 exam with flying colors. You must try PassSureExam PSE-Strata-Pro-24 exam questions today.

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q26-Q31):

NEW QUESTION # 26

A prospective customer has provided specific requirements for an upcoming firewall purchase, including the need to process a minimum of 200,000 connections per second while maintaining at least 15 Gbps of throughput with App-ID and Threat Prevention enabled.

What should a systems engineer do to determine the most suitable firewall for the customer?

- **A. Download the firewall sizing tool from the Palo Alto Networks support portal.**
- B. Upload 30 days of customer firewall traffic logs to the firewall calculator tool on the Palo Alto Networks support portal.
- C. Use the product selector tool available on the Palo Alto Networks website.
- D. Use the online product configurator tool provided on the Palo Alto Networks website.

Answer: A

Explanation:

* Firewall Sizing Tool (Answer B):

* The firewall sizing tool is the most accurate way to determine the suitable firewall model based on specific customer requirements, such as throughput, connections per second, and enabled features like App-ID and Threat Prevention.

* By inputting traffic patterns, feature requirements, and performance needs, the sizing tool provides tailored recommendations.

* Why Not A:

* While uploading traffic logs to the calculator tool may help analyze traffic trends, it is not the primary method for determining firewall sizing.

* Why Not C or D:

* The product configurator tool and product selector tool are not designed for detailed performance analysis based on real-world requirements like connections per second or enabled features.

References from Palo Alto Networks Documentation:

* Firewall Sizing Guide

NEW QUESTION # 27

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. Advanced Routing Engine
- **B. Parallel Processing**

- C. Management Data Plane Separation
- D. Single Pass Architecture

Answer: B,D

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.

NEW QUESTION # 28

Device-ID can be used in which three policies? (Choose three.)

- A. Security
- B. Decryption
- C. Policy-based forwarding (PBF)
- D. Quality of Service (QoS)
- E. SD-WAN

Answer: A,C,D

Explanation:

Device-ID is a feature in Palo Alto Networks firewalls that identifies devices based on their unique attributes (e.g., MAC addresses, device type, operating system). Device-ID can be used in several policy types to provide granular control. Here's how it applies to each option:

* Option A: Security

* Device-ID can be used in Security policies to enforce rules based on the device type or identity.

For example, you can create policies that allow or block traffic for specific device types (e.g., IoT devices).

* This is correct.

* Option B: Decryption

* Device-ID cannot be used in decryption policies. Decryption policies are based on traffic types, certificates, and other SSL/TLS attributes, not device attributes.

* This is incorrect.

* Option C: Policy-based forwarding (PBF)

* Device-ID can be used in PBF policies to control the forwarding of traffic based on the identified device. For example, you can route traffic from certain device types through specific ISPs or VPN tunnels.

* This is correct.

* Option D: SD-WAN

* SD-WAN policies use metrics such as path quality (e.g., latency, jitter) and application information for traffic steering. Device-ID is not a criterion used in SD-WAN policies.

* This is incorrect.

* Option E: Quality of Service (QoS)

* Device-ID can be used in QoS policies to apply traffic shaping or bandwidth control for specific devices. For example, you can prioritize or limit bandwidth for traffic originating from IoT devices or specific endpoints.

* This is correct.

References:

- * Palo Alto Networks documentation on Device-ID

NEW QUESTION # 29

Which two tools should a systems engineer use to showcase the benefit of an evaluation that a customer has just concluded?

- A. Security Lifecycle Review (SLR)
- B. Best Practice Assessment (BPA)
- C. Golden Images
- D. Firewall Sizing Guide

Answer: A,B

Explanation:

After a customer has concluded an evaluation of Palo Alto Networks solutions, it is critical to provide a detailed analysis of the results and benefits gained during the evaluation. The following two tools are most appropriate:

* Why "Best Practice Assessment (BPA)" (Correct Answer A)?The BPA evaluates the customer's firewall configuration against Palo Alto Networks' recommended best practices. It highlights areas where the configuration could be improved to strengthen security posture. This is an excellent tool to showcase how adopting Palo Alto Networks' best practices aligns with industry standards and improves security performance.

* Why "Security Lifecycle Review (SLR)" (Correct Answer B)?The SLR provides insights into the customer's security environment based on data collected during the evaluation. It identifies vulnerabilities, risks, and malicious activities observed in the network and demonstrates how Palo Alto Networks' solutions can address these issues. SLR reports use clear visuals and metrics, making it easier to showcase the benefits of the evaluation.

* Why not "Firewall Sizing Guide" (Option C)?The Firewall Sizing Guide is a pre-sales tool used to recommend the appropriate firewall model based on the customer's network size, performance requirements, and other criteria. It is not relevant for showcasing the benefits of an evaluation.

* Why not "Golden Images" (Option D)?Golden Images refer to pre-configured templates for deploying firewalls in specific use cases. While useful for operational efficiency, they are not tools for demonstrating the outcomes or benefits of a customer evaluation.

NEW QUESTION # 30

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

- A. High Risk
- B. Scanning Activity
- C. Command and Control
- D. Ransomware

Answer: D

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.

• • • • •

Valid PSE-Strata-Pro-24 Test Online: <https://www.passsureexam.com/PSE-Strata-Pro-24-pass4sure-exam-dumps.html>

- 2026 Latest PassSureExamPSE-Strata-Pro-24 PDF Dumps and PSE-Strata-Pro-24 Exam Engine Free Share:
<https://drive.google.com/open?id=1X7UgZBqfZ-fBV9A1KuFJAhtYL1mPFy3x>