

PSE-Strata-Pro-24 Test Guide Online & PSE-Strata-Pro-24 Latest Cram Materials



P.S. Free & New PSE-Strata-Pro-24 dumps are available on Google Drive shared by ValidTorrent: <https://drive.google.com/open?id=13Qryg3-jzwvTJaN5mAOB5OdLhztIA2S>

By contrasting with other products in the industry, our PSE-Strata-Pro-24 test guide really has a higher pass rate, which has been verified by many users. As long as you use our PSE-Strata-Pro-24 exam training I believe you can pass the exam. If you fail to pass the exam, we will give a full refund. PSE-Strata-Pro-24 learning guide hopes to progress together with you and work together for their own future. The high passing rate of Palo Alto Networks Systems Engineer Professional - Hardware Firewall exam training guide also requires your efforts. If you choose PSE-Strata-Pro-24 test guide, I believe we can together contribute to this high pass rate.

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

Topic	Details
Topic 1	<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 2	<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 3	<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 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 Test Guide Online <<

Pass Guaranteed 2026 Palo Alto Networks PSE-Strata-Pro-24: Palo Alto Networks Systems Engineer Professional - Hardware Firewall –Trustable Test Guide Online

The purpose of our product is to let the clients master the PSE-Strata-Pro-24 quiz torrent and not for other illegal purposes. Our system is well designed and any person or any organization has no access to the information of the clients. So please believe that we not only provide the best PSE-Strata-Pro-24 test prep but also provide the best privacy protection. Take it easy. If you really intend to pass the PSE-Strata-Pro-24 Exam, our software will provide you the fast and convenient learning and you will get the best study materials and get a very good preparation for the exam. The content of the PSE-Strata-Pro-24 guide torrent is easy to be mastered and has simplified the important information.

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q58-Q63):

NEW QUESTION # 58

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. AI Access Security
- C. Advanced Threat Prevention
- **D. Advanced WildFire**

Answer: D

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 # 59

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

Answer: B

Explanation:

* DNS Security (Answer C):

* DNS Security is the appropriate subscription for addressing threats over port 53.

* DNS tunneling is a common method used for data exfiltration, infiltration, and C2 activities, as it allows malicious traffic to be hidden within legitimate DNS queries.

* The DNS Security service applies machine learning models to analyze DNS queries 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 address DNS-based tunneling or 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 blocking DNS tunneling or 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 the DNS Security subscription, which specializes in DNS-layer threats.

References from Palo Alto Networks Documentation:

* DNS Security Subscription Overview

NEW QUESTION # 60

Which three descriptions apply to a perimeter firewall? (Choose three.)

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

Answer: B,D,E

Explanation:

A perimeter firewall is 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 provide network layer protection by 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 with data center firewalls, which monitor 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 secures north-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 in guarding 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

NEW QUESTION # 61

What would make a customer choose an on-premises solution over a cloud-based SASE solution for their network?

- **A. Most employees and applications in close physical proximity in a geographic region.**
- B. Hybrid work and cloud adoption at various locations that have different requirements per site.
- C. The need to enable business to securely expand its geographical footprint.
- D. High growth phase with existing and planned mergers, and with acquisitions being integrated.

Answer: A

Explanation:

SASE (Secure Access Service Edge) is a cloud-based solution that combines networking and security capabilities to address modern enterprise needs. However, there are scenarios where an on-premises solution is more appropriate.

A: High growth phase with existing and planned mergers, and with acquisitions being integrated.

This scenario typically favors a SASE solution since it provides flexible, scalable, and centralized security that is ideal for integrating newly acquired businesses.

B: Most employees and applications in close physical proximity in a geographic region.

This scenario supports the choice of an on-premises solution. When employees and applications are concentrated in a single geographic region, traditional on-premises firewalls and centralized security appliances provide cost-effective and efficient protection without the need for distributed, cloud-based infrastructure.

C: Hybrid work and cloud adoption at various locations that have different requirements per site.

This scenario aligns with a SASE solution. Hybrid work and varying site requirements are better addressed by SASE's ability to provide consistent security policies regardless of location.

D: The need to enable business to securely expand its geographical footprint.

Expanding into new geographic areas benefits from the scalability and flexibility of a SASE solution, which can deliver consistent security globally without requiring physical appliances at each location.

Key Takeaways:

* On-premises solutions are ideal for geographically concentrated networks with minimal cloud adoption.

* SASE is better suited for hybrid work, cloud adoption, and distributed networks.

References:

* Palo Alto Networks SASE Overview

* On-Premises vs. SASE Deployment Guide

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

Answer: D

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.

