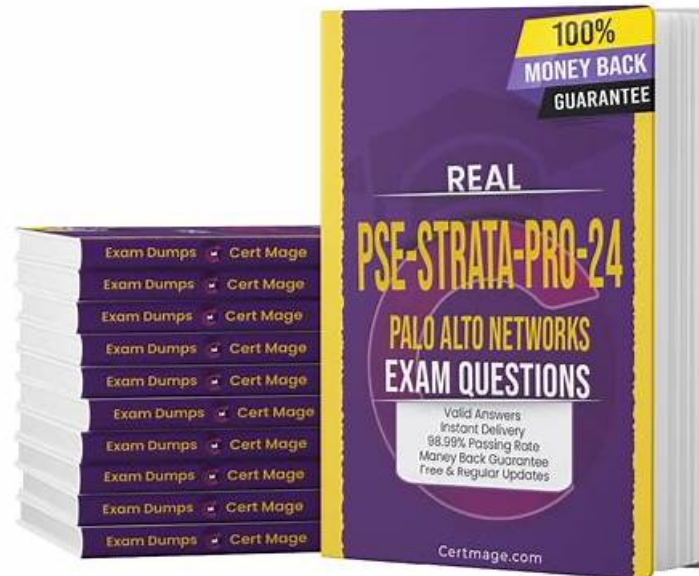


# PSE-Strata-Pro-24 Study Dumps, New PSE-Strata-Pro-24 Test Tutorial



BONUS!!! Download part of DumpTorrent PSE-Strata-Pro-24 dumps for free: <https://drive.google.com/open?id=16uwaWOO6PP7tkzbJKCQQN0UQBduH7v4>

These Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) practice test questions are customizable and give real Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) exam experience. Windows computers support desktop software. The web-based PSE-Strata-Pro-24 Practice Exam is supported by all browsers and operating systems.

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

Topic	Details
Topic 1	<ul style="list-style-type: none"><li>• 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.</li></ul>
Topic 2	<ul style="list-style-type: none"><li>• 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.</li></ul>
Topic 3	<ul style="list-style-type: none"><li>• 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.</li></ul>

Topic 4	<ul style="list-style-type: none"> <li>• <b>Business Value and Competitive Differentiators:</b> 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.</li> </ul>
---------	--

>> PSE-Strata-Pro-24 Study Dumps <<

## New Palo Alto Networks PSE-Strata-Pro-24 Test Tutorial & Free PSE-Strata-Pro-24 Download Pdf

Our company is considerably cautious in the selection of talent and always hires employees with store of specialized knowledge and skills on our PSE-Strata-Pro-24 exam questions. All the members of our experts and working staff maintain a high sense of responsibility, which is why there are so many people choose our PSE-Strata-Pro-24 Exam Materials and to be our long-term partner. For we carry forward the spirit of "firm & indomitable, developing & innovative, achieving the first class", serving customers with all our heart and soul with our wonderful PSE-Strata-Pro-24 practice braindumps.

### Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q35-Q40):

#### NEW QUESTION # 35

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

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

**Answer: C,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 North-South Traffic Control

#### NEW QUESTION # 36

A large global company plans to acquire 500 NGFWs to replace its legacy firewalls and has a specific requirement for centralized logging and reporting capabilities.

What should a systems engineer recommend?

- A. Highlight the efficiency of PAN-OS, which employs AI to automatically extract critical logs and generate daily executive

reports, and confirm that the purchase of 500 NGFWs is sufficient.

- **B. Combine Panorama for firewall management with Palo Alto Networks' cloud-based Strata Logging Service to offer scalability for the company's logging and reporting infrastructure.**
- C. Deploy a pair of M-1000 log collectors in the customer data center, and route logs from all 500 firewalls to the log collectors for centralized logging and reporting.
- D. Use Panorama for firewall management and to transfer logs from the 500 firewalls directly to a third-party SIEM for centralized logging and reporting.

**Answer: B**

Explanation:

A large deployment of 500 firewalls requires a scalable, centralized logging and reporting infrastructure.

Here's the analysis of each option:

\* Option A: Combine Panorama for firewall management with Palo Alto Networks' cloud-based Strata Logging Service to offer scalability for the company's logging and reporting infrastructure

\* The Strata Logging Service (or Cortex Data Lake) is a cloud-based solution that offers massive scalability for logging and reporting. Combined with Panorama, it allows for centralized log collection, analysis, and policy management without the need for extensive on-premises infrastructure.

\* This approach is ideal for large-scale environments like the one described in the scenario, as it ensures cost-effectiveness and scalability.

\* This is the correct recommendation.

\* Option B: Use Panorama for firewall management and to transfer logs from the 500 firewalls directly to a third-party SIEM for centralized logging and reporting

\* While third-party SIEM solutions can be integrated with Palo Alto Networks NGFWs, directly transferring logs from 500 firewalls to a SIEM can lead to bottlenecks and scalability issues.

Furthermore, relying on third-party solutions may not provide the same level of native integration as the Strata Logging Service.

\* This is not the ideal recommendation.

\* Option C: Highlight the efficiency of PAN-OS, which employs AI to automatically extract critical logs and generate daily executive reports, and confirm that the purchase of 500 NGFWs is sufficient

\* While PAN-OS provides AI-driven insights and reporting, this option does not address the requirement for centralized logging and reporting. It also dismisses the need for additional infrastructure to handle logs from 500 firewalls.

\* This is incorrect.

\* Option D: Deploy a pair of M-1000 log collectors in the customer data center, and route logs from all 500 firewalls to the log collectors for centralized logging and reporting

\* The M-1000 appliance is an on-premises log collector, but it has limitations in terms of scalability and storage capacity when compared to cloud-based options like the Strata Logging Service. Deploying only two M-1000 log collectors for 500 firewalls would result in potential performance and storage challenges.

\* This is not the best recommendation.

References:

\* Palo Alto Networks documentation on Panorama

\* Strata Logging Service (Cortex Data Lake) overview in Palo Alto Networks Docs

## NEW QUESTION # 37

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.

### NEW QUESTION # 38

In which two locations can a Best Practice Assessment (BPA) report be generated for review by a customer?

(Choose two.)

- A. Strata Cloud Manager (SCM)
- B. PANW Partner Portal
- C. AIOps
- D. Customer Support Portal

**Answer: B,D**

Explanation:

The Best Practice Assessment (BPA) report evaluates firewall and Panorama configurations against Palo Alto Networks' best practice recommendations. It provides actionable insights to improve the security posture of the deployment. BPA reports can be generated from the following locations:

\* Why "PANW Partner Portal" (Correct Answer A)? Partners with access to the Palo Alto Networks Partner Portal can generate BPA reports for customers as part of their service offerings. This allows partners to assess and demonstrate compliance with best practices.

\* Why "Customer Support Portal" (Correct Answer B)? Customers can log in to the Palo Alto Networks Customer Support Portal to generate their own BPA reports. This enables organizations to self-assess and improve their firewall configurations.

\* Why not "AIOps" (Option C)? While AIOps provides operational insights and best practice recommendations, it does not generate full BPA reports. BPA and AIOps are distinct tools within the Palo Alto Networks ecosystem.

\* Why not "Strata Cloud Manager (SCM)" (Option D)? Strata Cloud Manager is designed for managing multiple Palo Alto Networks cloud-delivered services and NGFWs but does not currently support generating BPA reports. BPA is limited to the Partner Portal and Customer Support Portal.

### NEW QUESTION # 39

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. Advanced Routing Engine
- C. Management Data Plane Separation
- D. Single Pass Architecture

**Answer: C,D**

Explanation:

\* Single Pass Architecture (Answer C):

\* Palo Alto Networks firewalls use Single Pass Architecture, meaning the firewall processes traffic once for all enabled security services.

\* This avoids duplicating inspection processes for multiple services like Threat Prevention, URL Filtering, and WildFire.

\* With a single traffic inspection pass, the firewall applies all security policies without degrading performance, even as additional CDSS subscriptions are enabled.

\* Management Data Plane Separation (Answer D):

\* The Management Plane and Data Plane are separated on Palo Alto Networks firewalls.

- [illegible]

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, dorahacks.io, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw,  
www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New PSE-Strata-Pro-24 dumps are available on Google Drive shared by DumpTorrent:  
<https://drive.google.com/open?id=16uwaWOO6PP7tkzbJKCQQN0UQBdUth7v4>