

検証するPSE-Strata-Pro-24合格受験記 |最初の試行で簡単に勉強して試験に合格する &公認されたPSE-Strata-Pro-24: Palo Alto Networks Systems Engineer Professional - Hardware Firewall



2025年Japancertの最新PSE-Strata-Pro-24 PDFダンプおよびPSE-Strata-Pro-24試験エンジンの無料共有: <https://drive.google.com/open?id=1-IGZO4iLLP9aw3QhUgPHrOtVEaX4X-z>

安全で信頼できるウェブサイトとして、あなたの個人情報の隠しとお支払いの安全性を保障していますから、弊社のPalo Alto NetworksのPSE-Strata-Pro-24試験ソフトを安心にお買いください。我々は一番全面的な問題集を提供しています。Japancertのサイトで探したり、弊社の係員に問い合わせたりすることができます。我々は試験の合格を保証することができます。

Palo Alto Networks PSE-Strata-Pro-24 認定試験の出題範囲:

トピック	出題範囲
トピック 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.
トピック 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.
トピック 3	<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.

トピック 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合格受験記 <<

試験の準備方法-素晴らしいPSE-Strata-Pro-24合格受験記試験-正確なPSE-Strata-Pro-24問題サンプル

成功の秘訣は目的への不変です。試験に合格し、認定を取得することが目的の場合。PSE-Strata-Pro-24試験クラムPDFは、試験の正しいショートカットになります。目標を達成する可能性や方法を逃さないでください。特に、PSE-Strata-Pro-24試験のクラムPDFには常に100%の合格率があります。ほとんどの場合、選択は努力よりも重要です。テストのきちんとした準備は、多くの時間を節約するのに役立ちます。Palo Alto Networks PSE-Strata-Pro-24試験クラムPDFは、間違いなく今後の試験に役立つでしょう。

Palo Alto Networks Systems Engineer Professional - Hardware Firewall 認定 PSE-Strata-Pro-24 試験問題 (Q60-Q65):

質問 # 60

According to a customer's CIO, who is upgrading PAN-OS versions, "Finding issues and then engaging with your support people requires expertise that our operations team can better utilize elsewhere on more valuable tasks for the business." The upgrade project was initiated in a rush because the company did not have the appropriate tools to indicate that their current NGFWs were reaching capacity.

Which two actions by the Palo Alto Networks team offer a long-term solution for the customer? (Choose two.)

- **A. Propose AIOps Premium within Strata Cloud Manager (SCM) to address the company's issues from within the existing technology.**
- B. Inform the CIO that the new enhanced security features they will gain from the PAN-OS upgrades will fix any future problems with upgrading and capacity.
- C. Recommend that the operations team use the free machine learning-powered AIOps for NGFW tool.
- **D. Suggest the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls.**

正解: A、D

解説:

The customer's CIO highlights two key pain points: (1) the operations team lacks expertise to efficiently manage PAN-OS upgrades and support interactions, diverting focus from valuable tasks, and (2) the company lacked tools to monitor NGFW capacity, leading to a rushed upgrade. The goal is to recommend long-term solutions leveraging Palo Alto Networks' offerings for Strata Hardware Firewalls. Options B and D-training and AIOps Premium within Strata Cloud Manager (SCM)- address these issues by enhancing team capability and providing proactive management tools. Below is a detailed explanation, verified against official documentation.

Step 1: Analyzing the Customer's Challenges

* **Expertise Gap:** The CIO notes that identifying issues and engaging support requires expertise the operations team doesn't fully have or can't prioritize. Upgrading PAN-OS on Strata NGFWs involves tasks like version compatibility checks, pre-upgrade validation, and troubleshooting, which demand familiarity with PAN-OS tools and processes.

* **Capacity Visibility:** The rushed upgrade stemmed from not knowing the NGFWs were nearing capacity (e.g., CPU, memory, session limits), indicating a lack of monitoring or predictive analytics.

Long-term solutions must address both operational efficiency and proactive capacity management, aligning with Palo Alto Networks' ecosystem for Strata firewalls.

Reference: PAN-OS Administrator's Guide (11.1) - Upgrade Overview

"Successful upgrades require planning, validation, and monitoring to avoid disruptions and ensure capacity is sufficient." Step 2:

Evaluating the Recommended Actions Option A: Recommend that the operations team use the free machine learning-powered AIOps for NGFW tool.

Analysis: AIOps for NGFW (free version) is a cloud-based tool that uses machine learning to monitor firewall health, detect

anomalies, and provide upgrade recommendations. It offers basic telemetry (e.g., CPU usage, session counts) and alerts, which could have flagged capacity issues earlier. However, it lacks advanced features like automated remediation, detailed capacity planning, or integration with Strata Cloud Manager, limiting its long-term impact. Additionally, it doesn't address the expertise gap, as the team still needs knowledge to interpret and act on insights.

Conclusion: Helpful but not a comprehensive long-term solution.

Reference: AIOps for NGFW Documentation

"The free version provides basic health monitoring and ML-driven insights but lacks premium features for proactive management."

Option B: Suggest the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls.

Analysis: Palo Alto Networks offers training through the Palo Alto Networks Authorized Training Partners and Cybersecurity Academy, covering PAN-OS administration, upgrades, and troubleshooting. For Strata NGFWs, courses like "Firewall Essentials: Configuration and Management (EDU-210)" teach upgrade best practices, capacity monitoring (e.g., via Device > High Availability > Resources), and support engagement.

How It Solves the Issue:

Reduces reliance on external expertise by upskilling the team.

Enables efficient upgrade planning (e.g., using Best Practice Assessment (BPA) tool).

Frees the team for higher-value tasks by minimizing support escalations.

Long-Term Benefit: A trained team can proactively manage upgrades and capacity, addressing the CIO's concern about expertise allocation.

Conclusion: A strong long-term solution.

Reference: Palo Alto Networks Training Catalog

"Training empowers operations teams to confidently manage NGFWs, including upgrades and capacity planning." Option C: Inform the CIO that the new enhanced security features they will gain from the PAN-OS upgrades will fix any future problems with upgrading and capacity.

Analysis: New PAN-OS versions (e.g., 11.1) bring features like enhanced App-ID, decryption, or ML-based threat detection, improving security. However, these don't inherently solve upgrade complexity or capacity visibility. Capacity issues depend on hardware limits (e.g., PA-5200 Series max sessions), not software features, and upgrades still require expertise. This response oversells benefits without addressing root causes.

Conclusion: Not a valid long-term solution.

Reference: PAN-OS 11.1 Release Notes

"New features enhance security but do not automate upgrade processes or capacity monitoring." Option D: Propose AIOps Premium within Strata Cloud Manager (SCM) to address the company's issues from within the existing technology.

Analysis: AIOps Premium, integrated with Strata Cloud Manager (SCM), is a subscription-based service for managing Strata NGFWs. It provides:

Predictive Analytics: Forecasts capacity needs (e.g., CPU, memory, sessions) using ML.

Upgrade Planning: Recommends optimal upgrade paths and validates configurations.

Proactive Alerts: Identifies issues before they escalate, reducing support calls.

Centralized Management: Monitors all firewalls from SCM, integrating with existing PAN-OS deployments.

How It Solves the Issue:

Prevents rushed upgrades by predicting capacity limits (e.g., via Capacity Saturation Reports).

Simplifies upgrade preparation with automated insights, reducing expertise demands.

Aligns with existing Strata technology, enhancing ROI.

Long-Term Benefit: Offers a scalable, proactive toolset to manage NGFWs, addressing both capacity and operational efficiency.

Conclusion: A robust long-term solution.

Reference: Strata Cloud Manager AIOps Premium Documentation

"AIOps Premium provides advanced capacity planning and upgrade readiness, minimizing operational burden." Step 3: Why B and D Are the Best Choices

B (Training): Directly tackles the expertise gap, empowering the team to handle upgrades and capacity monitoring independently. It's a foundational fix, ensuring long-term self-sufficiency.

D (AIOps Premium in SCM): Provides a technological solution to preempt capacity issues and streamline upgrades, reducing the need for deep expertise and support escalations. It complements training by automating complex tasks.

Synergy: Together, they address both human (expertise) and systemic (tools) challenges, aligning with the CIO's goals of operational efficiency and business value.

Step 4: How These Actions Integrate with Strata NGFWs

Training: Teaches use of PAN-OS tools like System Resources (CLI: show system resources) and Dynamic Updates for capacity and upgrade prep.

AIOps Premium: Enhances Strata NGFW management via SCM, pulling telemetry (e.g., from Device > Setup > Telemetry) to predict and resolve issues.

Reference: PAN-OS Administrator's Guide (11.1) - Monitoring

"Combine training and tools like AIOps to optimize NGFW performance and upgrades."

質問 # 61

What are two methods that a NGFW uses to determine if submitted credentials are valid corporate credentials? (Choose two.)

- A. LDAP query
- B. WMI client probing
- C. Group mapping
- D. Domain credential filter

正解: C、D

質問 # 62

A systems engineer (SE) has joined a team to work with a managed security services provider (MSSP) that is evaluating PAN-OS for edge connections to their customer base. The MSSP is concerned about how to efficiently handle routing with all of its customers, especially how to handle BGP peering, because it has created a standard set of rules and settings that it wants to apply to each customer, as well as to maintain and update them. The solution requires logically separated BGP peering setups for each customer. What should the SE do to increase the probability of Palo Alto Networks being awarded the deal?

- A. Collaborate with the MSSP to create an API call with a standard set of routing filters, maps, and related actions, then the MSSP can call the API whenever they bring on a new customer.
- B. Work with the MSSP to plan for the enabling of logical routers in the PAN-OS Advanced Routing Engine to allow sharing of routing profiles across the logical routers.
- C. Establish with the MSSP the use of vsys as the better way to segregate their environment so that customer data does not intermingle.
- D. Confirm to the MSSP that the existing virtual routers will allow them to have logically separated BGP peering setups, but that there is no method to handle the standard criteria across all of the routers.

正解: B

解説:

To address the MSSP's requirement for logically separated BGP peering setups while efficiently managing standard routing rules and updates, Palo Alto Networks offers the Advanced Routing Engine introduced in PAN-OS 11.0. The Advanced Routing Engine enhances routing capabilities, including support for logical routers, which is critical in this scenario.

Why A is Correct

- * Logical routers enable the MSSP to create isolated BGP peering configurations for each customer.
- * The Advanced Routing Engine allows the MSSP to share standard routing profiles (such as filters, policies, or maps) across logical routers, simplifying the deployment and maintenance of routing configurations.
- * This approach ensures scalability, as each logical router can handle the unique needs of a customer while leveraging shared routing rules.

Why Other Options Are Incorrect

- * B: While using APIs to automate deployment is beneficial, it does not solve the need for logically separated BGP peering setups. Logical routers provide this separation natively.
- * C: While virtual routers in PAN-OS can separate BGP peering setups, they do not support the efficient sharing of standard routing rules and profiles across multiple routers.
- * D: Virtual systems (vsys) are used to segregate administrative domains, not routing configurations. Vsys is not the appropriate solution for managing BGP peering setups across multiple customers.

Key Takeaways:

- * PAN-OS Advanced Routing Engine with logical routers simplifies BGP peering management for MSSPs.
- * Logical routers provide the separation required for customer environments while enabling shared configuration profiles.

References:

Palo Alto Networks PAN-OS 11.0 Advanced Routing Documentation

質問 # 63

Which two actions should a systems engineer take when a customer is concerned about how to remain aligned to Zero Trust principles as they adopt additional security features over time? (Choose two)

- A. Apply decryption where possible to inspect and log all new and existing traffic flows.
- B. Use the Policy Optimizer tool to understand security rules allowing users to bypass decryption.
- C. Use the Best Practice Assessment (BPA) tool to measure progress toward Zero Trust principles.
- D. Turn on all licensed Cloud-Delivered Security Services (CDSS) subscriptions in blocking mode for all policies.

正解: A、C

解説:

When adopting additional security features over time, remaining aligned with Zero Trust principles requires a focus on constant visibility, control, and adherence to best practices. The following actions are the most relevant:

* Why "Apply decryption where possible to inspect and log all new and existing traffic flows" (Correct Answer B)? Zero Trust principles emphasize visibility into all traffic, whether encrypted or unencrypted. Without decryption, encrypted traffic becomes a blind spot, which attackers can exploit.

By applying decryption wherever feasible, organizations ensure they can inspect, log, and enforce policies on encrypted traffic, thus adhering to Zero Trust principles.

* Why "Use the Best Practice Assessment (BPA) tool to measure progress toward Zero Trust principles" (Correct Answer C)? The BPA tool provides detailed insights into the customer's security configuration, helping measure alignment with Palo Alto Networks' Zero Trust best practices. It identifies gaps in security posture and recommends actionable steps to strengthen adherence to Zero Trust principles over time.

* Why not "Turn on all licensed Cloud-Delivered Security Services (CDSS) subscriptions in blocking mode for all policies" (Option A)? While enabling CDSS subscriptions (like Threat Prevention, URL Filtering, Advanced Threat Prevention) in blocking mode can enhance security, it is not an action specifically tied to maintaining alignment with Zero Trust principles. A more holistic approach, such as decryption and BPA analysis, is critical to achieving Zero Trust.

* Why not "Use the Policy Optimizer tool to understand security rules allowing users to bypass decryption" (Option D)? Policy Optimizer is used to optimize existing security rules by identifying unused or overly permissive policies. While useful, it does not directly address alignment with Zero Trust principles or help enforce decryption.

質問 # 64

A systems engineer (SE) successfully demonstrates NGFW managed by Strata Cloud Manager (SCM) to a company. In the resulting planning phase of the proof of value (POV), the CISO requests a test that shows how the security policies are either meeting, or are progressing toward meeting, industry standards such as Critical Security Controls (CSC), and how the company can verify that it is effectively utilizing the functionality purchased.

During the POV testing timeline, how should the SE verify that the POV will meet the CISO's request?

- A. At the beginning, work with the customer to create custom dashboards and reports for any information required, so reports can be pulled as needed by the customer.
- B. At the beginning, use PANhandler golden images that are designed to align to compliance and to turning on the features for the CDSS subscription being tested.
- **C. Near the end, pull a Security Lifecycle Review (SLR) in the POV and create a report for the customer.**
- D. Near the end, the customer pulls information from these SCM dashboards: Best Practices, CDSS Adoption, and NGFW Feature Adoption.

正解: C

解説:

* Security Lifecycle Review (SLR) (Answer A):

* The Security Lifecycle Review (SLR) is a detailed report generated by Palo Alto Networks firewalls that provides visibility into application usage, threats, and policy alignment with industry standards.

* During the POV, running an SLR near the end of the timeline allows the customer to see:

* How well their current security policies align with Critical Security Controls (CSC) or other industry standards.

* Insights into application usage and threats discovered during the POV.

* This provides actionable recommendations for optimizing policies and ensuring the purchased functionality is being effectively utilized.

* Why Not B:

* While creating custom dashboards and reports at the beginning might provide useful insights, the question focuses on verifying progress toward meeting CSC standards. This is specifically addressed by the SLR, which is designed to measure and report on such criteria.

* Why Not C:

* Pulling information from SCM dashboards like Best Practices and Feature Adoption can help assess firewall functionality but may not provide a comprehensive review of compliance or CSC alignment, as the SLR does.

* Why Not D:

* While PANhandler golden images can help configure features in alignment with specific subscriptions or compliance goals, they are primarily used to deploy predefined templates, not to assess security policy effectiveness or compliance with CSC standards.

References from Palo Alto Networks Documentation:

* Security Lifecycle Review Overview

P.S.JapancertがGoogle Driveで共有している無料の2025 Palo Alto Networks PSE-Strata-Pro-24ダ
ンプ: <https://drive.google.com/open?id=1-IGZO4iLLiP9aw3QhUgPHrOtVEaX4X-z>