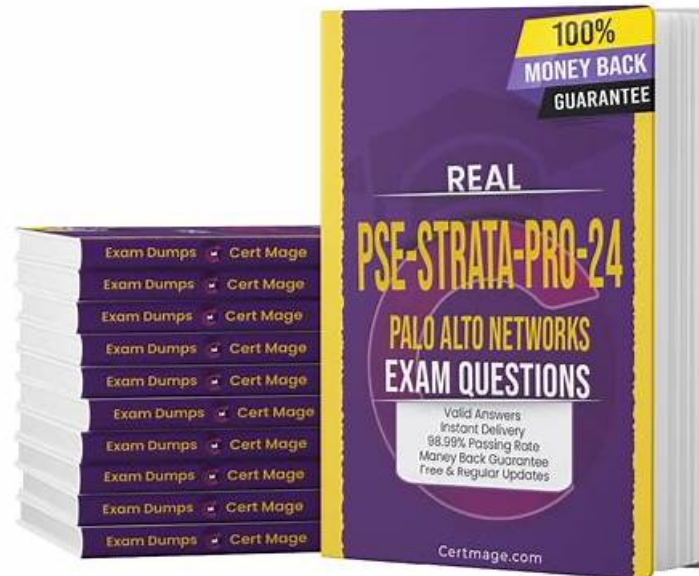


# New PSE-Strata-Pro-24 Braindumps Pdf & Exam PSE-Strata-Pro-24 Vce Format



BTW, DOWNLOAD part of RealVCE PSE-Strata-Pro-24 dumps from Cloud Storage: <https://drive.google.com/open?id=1yLdvonWkNPK8HhaF5Vn9WrLEY-Ykc4sr>

By taking our Palo Alto Networks PSE-Strata-Pro-24 practice exam, which is customizable, you can find and strengthen your weak areas. Additionally, we provide a specialized 24/7 customer support team to assist you with any problems you may run into while using our Palo Alto Networks Systems Engineer Professional - Hardware Firewall exam questions. Our Palo Alto Networks PSE-Strata-Pro-24 desktop-based practice exam software's ability to be used without an active internet connection is another incredible feature.

Under the hatchet of fast-paced development, we must always be cognizant of social long term goals and the direction of the development of science and technology. Adapt to the network society, otherwise, we will take the risk of being obsoleted. Although our PSE-Strata-Pro-24 exam dumps have been known as one of the world's leading providers of exam materials, you may be still suspicious of the content. For your convenience, we especially provide several demos for future reference and we promise not to charge you of any fee for those downloading. Therefore, we welcome you to download to try our PSE-Strata-Pro-24 Exam for a small part. Then you will know whether it is suitable for you to use our PSE-Strata-Pro-24 test questions. There are answers and questions provided to give an explicit explanation. We are sure to be at your service if you have any downloading problems.

>> New PSE-Strata-Pro-24 Braindumps Pdf <<

## Exam PSE-Strata-Pro-24 Vce Format & Online PSE-Strata-Pro-24 Training Materials

The 24/7 support team is just an e-mail away for our customers so that they can contact us anytime. Our team will solve all of their issues as quickly as possible. Free demos and up to 1 year of free updates of our Palo Alto Networks Exams are also available at RealVCE. Buy updated and Real PSE-Strata-Pro-24 Exam Questions now and earn your dream PSE-Strata-Pro-24 certification with RealVCE!

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

---

Topic	Details
Topic 1	<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 2	<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 3	<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 4	<ul style="list-style-type: none"> <li>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.</li> </ul>

## Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q47-Q52):

### NEW QUESTION # 47

Which two statements correctly describe best practices for sizing a firewall deployment with decryption enabled? (Choose two.)

- A. Perfect Forward Secrecy (PFS) ephemeral key exchange algorithms such as Diffie-Hellman Ephemeral (DHE) and Elliptic-Curve Diffie-Hellman Exchange (ECDHE) consume more processing resources than Rivest-Shamir-Adleman (RSA) algorithms.
- B. Rivest-Shamir-Adleman (RSA) certificate authentication method (not the RSA key exchange algorithm) consumes more resources than Elliptic Curve Digital Signature Algorithm (ECDSA), but ECDSA is more secure.
- C. SSL decryption traffic amounts vary from network to network.
- D. Large average transaction sizes consume more processing power to decrypt.

**Answer: A,C**

Explanation:

When planning a firewall deployment with SSL/TLS decryption enabled, it is crucial to consider the additional processing overhead introduced by decrypting and inspecting encrypted traffic. Here are the details for each statement:

- \* Why "SSL decryption traffic amounts vary from network to network" (Correct Answer A)? SSL decryption traffic varies depending on the organization's specific network environment, user behavior, and applications. For example, networks with heavy web traffic, cloud applications, or encrypted VoIP traffic will have more SSL/TLS decryption processing requirements. This variability means each deployment must be properly assessed and sized accordingly.
- \* Why "Perfect Forward Secrecy (PFS) ephemeral key exchange algorithms such as Diffie-Hellman Ephemeral (DHE) and Elliptic-Curve Diffie-Hellman Exchange (ECDHE) consume more processing resources than Rivest-Shamir-Adleman (RSA) algorithms" (Correct Answer C)? PFS algorithms like DHE and ECDHE generate unique session keys for each connection, ensuring better security but requiring significantly more processing power compared to RSA key exchange. When decryption is enabled, firewalls must handle these computationally expensive operations for every encrypted session, impacting performance and sizing requirements.
- \* Why not "Large average transaction sizes consume more processing power to decrypt" (Option B)? While large transaction sizes can consume additional resources, SSL/TLS decryption is more dependent on the number of sessions and the complexity of the encryption algorithms used, rather than the size of the transactions. Hence, this is not a primary best practice consideration.
- \* Why not "Rivest-Shamir-Adleman (RSA) certificate authentication method consumes more resources than Elliptic Curve Digital Signature Algorithm (ECDSA), but ECDSA is more secure" (Option D)? This statement discusses certificate authentication methods,

not SSL/TLS decryption performance. While ECDSA is more efficient and secure than RSA, it is not directly relevant to sizing considerations for firewall deployments with decryption enabled.

#### NEW QUESTION # 48

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. 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.
- B. Recommend that the operations team use the free machine learning-powered AIOps for NGFW tool.
- C. Suggest the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls.
- D. Propose AIOps Premium within Strata Cloud Manager (SCM) to address the company's issues from within the existing technology.

**Answer: C,D**

Explanation:

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."

## NEW QUESTION # 49

An existing customer wants to expand their online business into physical stores for the first time. The customer requires NGFWs at the physical store to handle SD-WAN, security, and data protection needs, while also mandating a vendor-validated deployment method. Which two steps are valid actions for a systems engineer to take? (Choose two.)

- A. Use the reference architecture "On-Premises Network Security for the Branch Deployment Guide" to achieve a desired architecture.
- B. Create a bespoke deployment plan with the customer that reviews their cloud architecture, store footprint, and security requirements.
- C. Use Golden Images and Day 1 configuration to create a consistent baseline from which the customer can efficiently work.
- D. Recommend the customer purchase Palo Alto Networks or partner-provided professional services to meet the stated requirements.

**Answer: A,D**

Explanation:

When an existing customer expands their online business into physical stores and requires Next-Generation Firewalls (NGFWs) at those locations to handle SD-WAN, security, and data protection-while mandating a vendor-validated deployment method-a systems engineer must leverage Palo Alto Networks' Strata Hardware Firewall capabilities and validated deployment strategies. The Strata portfolio, particularly the PA- Series NGFWs, is designed to secure branch offices with integrated SD-WAN and robust security features.

Below is a detailed explanation of why options A and D are the correct actions, grounded in Palo Alto Networks' documentation and practices as of March 08, 2025.

#### Step 1: Recommend Professional Services (Option A)

The customer's requirement for a "vendor-validated deployment method" implies a need for expertise and assurance that the solution meets their specific needs-SD-WAN, security, and data protection-across new physical stores. Palo Alto Networks offers professional services, either directly or through certified partners, to ensure proper deployment of Strata Hardware Firewalls like the PA-400 Series or PA-1400 Series, which are ideal for branch deployments. These services provide end-to-end support, from planning to implementation, aligning with the customer's mandate for a validated approach.

- \* Professional Services Scope: Palo Alto Networks' professional services include architecture design, deployment, and optimization for NGFWs and SD-WAN. This ensures that the PA-Series firewalls are configured to handle SD-WAN (e.g., dynamic path selection), security (e.g., Threat Prevention with ML-powered inspection), and data protection (e.g., WildFire for malware analysis and Data Loss Prevention integration).

- \* Vendor Validation: By recommending these services, the engineer ensures a deployment that adheres to Palo Alto Networks' best practices, meeting the customer's requirement for a vendor-validated method. This is particularly critical for a customer new to physical store deployments, as it mitigates risks and accelerates time-to-value.

- \* Strata Hardware Relevance: The PA-410, for example, is a desktop NGFW designed for small branch offices, offering SD-WAN and Zero Trust security out of the box. Professional services ensure its correct integration into the customer's ecosystem.

#### Reference:

"Palo Alto Networks Professional Services" documentation states, "Our experts help you design, deploy, and optimize your security architecture," covering NGFWs and SD-WAN for branch deployments.

"PA-400 Series" datasheet highlights its suitability for branch offices with "integrated SD-WAN functionality" and "advanced threat prevention," validated through professional deployment support.

Why Option A is Correct: Recommending professional services meets the customer's need for a vendor-validated deployment, leveraging Palo Alto Networks' expertise to tailor Strata NGFWs to the physical store requirements.

#### Step 2: Use the Reference Architecture Guide (Option D)

Explanation: Palo Alto Networks provides reference architectures, such as the "On-Premises Network Security for the Branch Deployment Guide," to offer vendor-validated blueprints for deploying Strata Hardware Firewalls in branch environments. This guide is specifically designed for scenarios like the customer's-expanding into physical stores-where SD-WAN, security, and data protection are critical.

Using this reference architecture ensures a consistent, proven deployment method that aligns with the customer's mandate.

Reference Architecture Details: The "On-Premises Network Security for the Branch Deployment Guide" outlines how to deploy PA-Series NGFWs with SD-WAN to secure branch offices. It includes configurations for secure connectivity (e.g., VPNs, SD-WAN hubs), threat prevention (e.g., App-ID, URL Filtering), and data protection (e.g., file blocking policies).

SD-WAN Integration: The guide leverages the PA-Series' native SD-WAN capabilities, such as dynamic path selection and application-based traffic steering, to optimize connectivity between stores and the existing online infrastructure.

Vendor Validation: As a Palo Alto Networks-authored document, this guide is inherently vendor-validated, providing step-by-step instructions and best practices that the engineer can adapt to the customer's store footprint.

Strata Hardware Relevance: The guide recommends models like the PA-1400 Series for larger branches or the PA-410 for smaller stores, ensuring scalability and consistency across deployments.

#### Reference:

"On-Premises Network Security for the Branch Deployment Guide" (Palo Alto Networks) details "branch office deployment with SD-WAN and NGFW capabilities," validated for Strata hardware like the PA-Series.

"SD-WAN Reference Architecture" complements this, emphasizing the PA-Series' role in "simplified branch deployments with integrated security." Why Option D is Correct: Using the reference architecture provides a vendor-validated, repeatable framework that directly addresses the customer's needs for SD-WAN, security, and data protection, ensuring a successful expansion into physical stores.

#### Why Other Options Are Incorrect

Option B: Use Golden Images and Day 1 configuration to create a consistent baseline from which the customer can efficiently work.

Analysis: While Golden Images and Day 1 configurations (e.g., via Panorama or Zero Touch Provisioning) are valuable for consistency and automation, they are not explicitly vendor-validated deployment methods in the context of Palo Alto Networks' documentation. These are tools for execution, not strategic actions for planning a deployment. Additionally, they assume prior planning, which isn't addressed here, making this less aligned with the customer's stated requirements.

Reference: "Panorama Administrator's Guide" mentions Golden Images for configuration consistency, but it's a technical implementation step, not a vendor-validated planning action.

Option C: Create a bespoke deployment plan with the customer that reviews their cloud architecture, store footprint, and security requirements.

Analysis: Creating a bespoke plan is a reasonable approach but does not inherently meet the "vendor-validated" mandate unless it leverages Palo Alto Networks' official tools (e.g., reference architectures or professional services). The question emphasizes a vendor-validated method, and a custom plan risks deviating from established, proven guidelines unless explicitly tied to such resources.

Reference: No specific Palo Alto Networks documentation mandates bespoke plans as a vendor-validated approach; instead, it



prioritizes reference architectures and professional services.

#### Conclusion

Options A and D are the most valid actions for a systems engineer addressing the customer's expansion into physical stores with Strata Hardware Firewalls. Recommending professional services (A) ensures expert-led, vendor-validated deployment, while using the "On-Premises Network Security for the Branch Deployment Guide" (D) provides a proven blueprint tailored to SD-WAN, security, and data protection needs. Together, these steps leverage the PA-Series' capabilities to deliver a secure, scalable solution for the customer's new physical infrastructure.

#### NEW QUESTION # 50

A customer claims that Advanced WildFire miscategorized a file as malicious and wants proof, because another vendor has said that the file is benign.

How could the systems engineer assure the customer that Advanced WildFire was accurate?

- A. Open a TAG ticket for the customer and allow support engineers to determine the appropriate action.
- B. Do nothing because the customer will realize Advanced WildFire is right.
- C. Review the threat logs for information to provide to the customer.
- **D. Use the WildFire Analysis Report in the log to show the customer the malicious actions the file took when it was detonated.**

#### Answer: D

##### Explanation:

Advanced WildFire is Palo Alto Networks' cloud-based malware analysis and prevention solution. It determines whether files are malicious by executing them in a sandbox environment and observing their behavior. To address the customer's concern about the file categorization, the systems engineer must provide evidence of the file's behavior. Here's the analysis of each option:

\* Option A: Review the threat logs for information to provide to the customer

\* Threat logs can provide a summary of events and verdicts for malicious files, but they do not include the detailed behavior analysis needed to convince the customer.

\* While reviewing the logs is helpful as a preliminary step, it does not provide the level of proof the customer needs.

\* This option is not sufficient on its own.

\* Option B: Use the WildFire Analysis Report in the log to show the customer the malicious actions the file took when it was detonated

\* WildFire generates an analysis report that includes details about the file's behavior during detonation in the sandbox, such as network activity, file modifications, process executions, and any indicators of compromise (IoCs).

\* This report provides concrete evidence to demonstrate why the file was flagged as malicious. It is the most accurate way to assure the customer that WildFire's decision was based on observed malicious actions.

\* This is the best option.

\* Option C: Open a TAG ticket for the customer and allow support engineers to determine the appropriate action

\* While opening a support ticket is a valid action for further analysis or appeal, it is not a direct way to assure the customer of the current WildFire verdict.

\* This option does not directly address the customer's request for immediate proof.

\* This option is not ideal.

\* Option D: Do nothing because the customer will realize Advanced WildFire is right

\* This approach is dismissive of the customer's concerns and does not provide any evidence to support WildFire's decision.

\* This option is inappropriate.

##### References:

\* Palo Alto Networks documentation on WildFire

\* WildFire Analysis Reports

#### NEW QUESTION # 51

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. Near the end, the customer pulls information from these SCM dashboards: Best Practices, CDSS Adoption, and NGFW Feature Adoption.
- C. 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.
- D. Near the end, pull a Security Lifecycle Review (SLR) in the POV and create a report for the customer.

**Answer: A**

Explanation:

The SE has demonstrated an NGFW managed by SCM, and the CISO now wants the POV to show progress toward industry standards (e.g., CSC) and verify effective use of purchased features (e.g., CDSS subscriptions like Advanced Threat Prevention). The SE must ensure the POV delivers measurable evidence during the testing timeline. Let's evaluate the options.

Step 1: Understand the CISO's Request

\* Industry Standards (e.g., CSC): The Center for Internet Security's Critical Security Controls (e.g., CSC 1: Inventory of Devices, CSC 4: Secure Configuration) require visibility, threat prevention, and policy enforcement, which NGFW and SCM can address.

\* Feature Utilization: Confirm that licensed functionalities (e.g., App-ID, Threat Prevention, URL Filtering) are active and effective.

\* POV Goal: Provide verifiable progress and utilization metrics within the testing timeline.

Reference: Strata Cloud Manager Overview ([docs.paloaltonetworks.com/strata-cloud-manager](https://docs.paloaltonetworks.com/strata-cloud-manager)); CIS Critical Security Controls ([www.cisecurity.org/controls](https://www.cisecurity.org/controls)).

Step 2: Define SCM Capabilities

Strata Cloud Manager (SCM): A cloud-based management platform for Palo Alto NGFWs, offering dashboards (e.g., Best Practices, Feature Adoption) and custom reporting to monitor security posture, policy compliance, and subscription usage.

Security Lifecycle Review (SLR): A report generated via the Customer Support Portal (not SCM) analyzing traffic logs for security gaps, not real-time POV progress.

Dashboards and Reports: SCM provides prebuilt and customizable views for real-time insights into policy effectiveness and feature adoption.

Reference: SCM Dashboards and Reports ([docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and-reports](https://docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and-reports)).

Step 3: Evaluate Each Option

A). Near the end, pull a Security Lifecycle Review (SLR) in the POV and create a report for the customer.

Description: The SLR analyzes 7-30 days of traffic logs, providing a retrospective security posture assessment (e.g., threats blocked, policy gaps).

Process: Near POV end, upload logs to the Customer Support Portal (Support > Security Lifecycle Review), generate, and share the report.

Limitations:

SLR is a point-in-time analysis, not a real-time progress tracker during the POV timeline.

Requires post-POV log collection, delaying feedback.

Doesn't directly show feature utilization progress or CSC alignment in SCM.

Fit: Misses the "during the POV timeline" requirement; better for post-POV analysis.

Reference: Security Lifecycle Review Guide ([support.paloaltonetworks.com](https://support.paloaltonetworks.com), requires login).

B). 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.

Description: SCM allows custom dashboards and reports (Monitor > Dashboards or Reports) tailored to metrics like policy compliance (CSC alignment) and feature usage (e.g., Threat Prevention hits).

Process:

At POV start, collaborate with the CISO to define metrics (e.g., "Threats blocked by ATP" for CSC 6, "App-ID usage" for feature adoption).

Configure custom dashboards in SCM (Dashboards > Add Dashboard > Custom).

Set up scheduled or on-demand reports (Reports > Custom Reports).

Enable the customer to monitor progress throughout the POV.

Benefits:

Real-time visibility into policy effectiveness and feature use during the timeline.

Aligns with CSC (e.g., blocked malware events) and shows subscription ROI.

Empowers the customer to verify results independently.

Fit: Meets the CISO's request fully within the POV timeline.

Reference: SCM Custom Dashboards ([docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and-reports/custom-dashboards](https://docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and-reports/custom-dashboards)).

C). Near the end, the customer pulls information from these SCM dashboards: Best Practices, CDSS Adoption, and NGFW Feature Adoption.

Description: SCM provides prebuilt dashboards:

Best Practices: Assesses policy alignment with security standards.

CDSS Adoption: Tracks subscription usage (e.g., ATP, URL Filtering).

NGFW Feature Adoption: Monitors features like App-ID or User-ID.

Limitations:

Waiting until "near the end" delays visibility, missing ongoing progress tracking.

Prebuilt dashboards may not fully align with CSC or specific customer needs without customization.

Fit: Useful but incomplete; lacks proactive setup and real-time monitoring throughout the POV.

Reference: SCM Prebuilt Dashboards ([docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and-reports/prebuilt-dashboards](https://docs.paloaltonetworks.com/strata-cloud-manager/dashboards-and-reports/prebuilt-dashboards)).

D). 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.

Description: PANhandler is a tool for managing Skillets (configuration templates), including "golden images" for compliance (e.g., NIST, CIS benchmarks).

Process: Apply a Skillet at POV start to configure the NGFW with compliance settings and CDSS features.

Limitations:

Configures the NGFW but doesn't verify progress or utilization during the POV.

No reporting or dashboard integration for the CISO to track results.

Fit: Sets up the environment but doesn't meet the verification requirement.

Reference: PANhandler Skillets ([github.com/PaloAltoNetworks/panhandler](https://github.com/PaloAltoNetworks/panhandler)).

Step 4: Select the Best Approach

B is the strongest choice:

Proactive: Starts at the beginning, ensuring metrics are tracked throughout the POV.

Customizable: Tailors dashboards/reports to CSC (e.g., threat detection for CSC 6) and feature use (e.g., ATP events).

Verifiable: Enables the customer to pull reports as needed, meeting the CISO's request within the timeline.

Why not A, C, or D?

A: SLR is retrospective, not real-time, missing the "during" aspect.

C: Prebuilt dashboards are helpful but delayed and less flexible than custom options.

D: Golden images configure but don't verify progress or utilization.

Step 5: Verification with Palo Alto Documentation

SCM Custom Dashboards: Supports real-time, tailored monitoring (SCM Docs).

SLR: Post-analysis tool, not POV-progressive (Support Portal Docs).

Prebuilt Dashboards: Limited customization (SCM Docs).

PANhandler: Configuration-focused, not reporting-focused (PANhandler Docs).

Thus, the verified answer is B.

## NEW QUESTION # 52

.....

Once you have used our PSE-Strata-Pro-24 exam training in a network environment, you no longer need an internet connection the next time you use it, and you can choose to use PSE-Strata-Pro-24 exam training at your own right. Our PSE-Strata-Pro-24 Exam Training do not limit the equipment, do not worry about the network, this will reduce you many learning obstacles, as long as you want to use PSE-Strata-Pro-24 test guide, you can enter the learning state.

**Exam PSE-Strata-Pro-24 Vce Format:** [https://www.realvce.com/PSE-Strata-Pro-24\\_free-dumps.html](https://www.realvce.com/PSE-Strata-Pro-24_free-dumps.html)

- PSE-Strata-Pro-24 Test Question ☐ Composite Test PSE-Strata-Pro-24 Price ☐ PSE-Strata-Pro-24 Reliable Study Questions ☐ Search for **【 PSE-Strata-Pro-24 】** and easily obtain a free download on ☐ [www.prepawayete.com](http://www.prepawayete.com) ☐ ☐ PSE-Strata-Pro-24 Training Questions
- 2026 Palo Alto Networks PSE-Strata-Pro-24 Fantastic New Braindumps Pdf ☐ Easily obtain free download of  $\Rightarrow$  PSE-Strata-Pro-24  $\Leftarrow$  by searching on ( [www.pdfvce.com](http://www.pdfvce.com) ) ☐ Valid PSE-Strata-Pro-24 Dumps Demo
- Composite Test PSE-Strata-Pro-24 Price ☐ Latest PSE-Strata-Pro-24 Exam Forum ☐ PSE-Strata-Pro-24 Exam Overviews ☐ Easily obtain free download of  $\Rightarrow$  PSE-Strata-Pro-24 ☐ by searching on  $\Rightarrow$  [www.torrentvce.com](http://www.torrentvce.com) ☐ ☐ ☐ Reliable PSE-Strata-Pro-24 Study Materials
- Pass PSE-Strata-Pro-24 Test ☐ PSE-Strata-Pro-24 Latest Test Bootcamp ☐ Pass PSE-Strata-Pro-24 Test ☐ Open ( [www.pdfvce.com](http://www.pdfvce.com) ) enter ☒ PSE-Strata-Pro-24 ☒ ☐ and obtain a free download ☐ PSE-Strata-Pro-24 Training Questions
- First-hand Palo Alto Networks New PSE-Strata-Pro-24 Braindumps Pdf: Palo Alto Networks Systems Engineer Professional - Hardware Firewall - Exam PSE-Strata-Pro-24 Vce Format ☐ Open ☐ [www.examcollectionpass.com](http://www.examcollectionpass.com) ☐ enter { PSE-Strata-Pro-24 } and obtain a free download ☐ New PSE-Strata-Pro-24 Exam Discount
- Valid PSE-Strata-Pro-24 Dumps Demo ☐ Composite Test PSE-Strata-Pro-24 Price ☐ PSE-Strata-Pro-24 Interactive Practice Exam ☐ Search for ☐ PSE-Strata-Pro-24 ☐ on ☐ [www.pdfvce.com](http://www.pdfvce.com) ☐ immediately to obtain a free download ☐ ☐ PSE-Strata-Pro-24 Reliable Study Questions



- Quiz High Hit-Rate Palo Alto Networks - New PSE-Strata-Pro-24 Braindumps Pdf □ Immediately open ➡ [www.prep4sures.top](http://www.prep4sures.top) □□□ and search for 【 PSE-Strata-Pro-24 】 to obtain a free download □PSE-Strata-Pro-24 Test Question
- 100% Pass 2026 PSE-Strata-Pro-24: The Best New Palo Alto Networks Systems Engineer Professional - Hardware Firewall Braindumps Pdf □ The page for free download of “PSE-Strata-Pro-24 ” on ➡ [www.pdfvce.com](http://www.pdfvce.com) □ will open immediately □Composite Test PSE-Strata-Pro-24 Price
- Use Palo Alto Networks PSE-Strata-Pro-24 PDF Questions To Get Better Results □ Open ▷ [www.prepawayete.com](http://www.prepawayete.com) ◁ enter ( PSE-Strata-Pro-24 ) and obtain a free download □Pass PSE-Strata-Pro-24 Test
- 2026 Palo Alto Networks PSE-Strata-Pro-24 Fantastic New Braindumps Pdf □ Simply search for 【 PSE-Strata-Pro-24 】 for free download on “ [www.pdfvce.com](http://www.pdfvce.com) ” □PSE-Strata-Pro-24 Exam Topics
- 2026 Palo Alto Networks PSE-Strata-Pro-24 Fantastic New Braindumps Pdf □ Download 「 PSE-Strata-Pro-24 」 for free by simply searching on ➡ [www.practicevce.com](http://www.practicevce.com) □ □PSE-Strata-Pro-24 Latest Test Bootcamp
- [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [study.stcs.edu.np](http://study.stcs.edu.np), [hub.asifulfat.com](http://hub.asifulfat.com), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [giphy.com](http://giphy.com), [bbs.t-firefly.com](http://bbs.t-firefly.com), [www.meilichina.com](http://www.meilichina.com), [bbs.t-firefly.com](http://bbs.t-firefly.com), [shortcourses.russellcollege.edu.au](http://shortcourses.russellcollege.edu.au), [www.academy.taffids.org](http://www.academy.taffids.org), Disposable vapes

2026 Latest RealVCE PSE-Strata-Pro-24 PDF Dumps and PSE-Strata-Pro-24 Exam Engine Free Share:

<https://drive.google.com/open?id=1yLdvnWkNPK8HhaF5Vn9WrLEY-Ykc4sr>