

PSE-Strata-Pro-24 exam practice material & PSE-Strata-Pro-24 study training pdf & PSE-Strata-Pro-24 online test engine



INTRODUCTION TO PSE-Strata-Pro-24 EXAM

Maximizing Your Success in the Palo-Alto-Networks PSE-Strata-Pro-24 Exam Questions is crucial for aspiring Azure Solutions Architects. This presentation will provide a comprehensive guide on utilizing Certs4Future exam dumps to enhance your preparation and boost your confidence. Let's explore effective strategies to ensure your success.



[LEARN MORE](#)

BTW, DOWNLOAD part of TestBraindump PSE-Strata-Pro-24 dumps from Cloud Storage: <https://drive.google.com/open?id=1CA4v0tRP3H5lahS9wq7Nmb7QBeQIA7hV>

The web-based Palo Alto Networks PSE-Strata-Pro-24 practice exam does not require special plugins and creates a PSE-Strata-Pro-24 testing atmosphere that removes candidates exam anxiety. "TestBraindump" web-based Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) practice test tracks your progress and helps you overcome mistakes. Our Palo Alto Networks PSE-Strata-Pro-24 practice exam software displays results at the end of each attempt.

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

Topic	Details
Topic 1	<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.
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"> • 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 4	<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.

Preparing Palo Alto Networks PSE-Strata-Pro-24 Exam is Easy with Our High-quality Reliable PSE-Strata-Pro-24 Exam Registration: Palo Alto Networks Systems Engineer Professional - Hardware Firewall

In light of the truth that different people have various learning habits, we launch three PSE-Strata-Pro-24 training questions versions for your guidance. In addition, you can freely download the demo of PSE-Strata-Pro-24 learning materials for your consideration. We promise there will be no extra charges for such a try, on the contrary, we sincerely suggest you to try the demos of our PSE-Strata-Pro-24 Exam Questions and make a well-content choice. You will find that our PSE-Strata-Pro-24 training guide is worthy to buy for you time and money!

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q34-Q39):

NEW QUESTION # 34

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

Answer: B,D

Explanation:

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.

Reference: Palo Alto Networks' Zero Trust documentation and Best Practice Assessment (BPA) confirm the importance of decryption and best practices in aligning with Zero Trust principles.

NEW QUESTION # 35

A systems engineer (SE) is working with a customer that is fully cloud-deployed for all applications. The customer is interested in Palo Alto Networks NGFWs but describes the following challenges:

"Our apps are in AWS and Azure, with whom we have contracts and minimum-revenue guarantees. We would use the built-in firewall on the cloud service providers (CSPs), but the need for centralized policy management to reduce human error is more important." Which recommendations should the SE make?

- A. Cloud NGFWs in AWS and VM-Series firewall in Azure; the customer selects a PAYG licensing Panorama deployment in their CSP of choice.

- B. VM-Series firewall and CN-Series firewall in both CSPs; provide the customer a private-offer Panorama virtual appliance from their CSP's marketplace of choice to centrally manage the systems.
- C. VM-Series firewalls in both CSPs; manually built Panorama in the CSP of choice on a host of either type: Palo Alto Networks provides a license.
- **D. Cloud NGFWs at both CSPs; provide the customer a license for a Panorama virtual appliance from their CSP's marketplace of choice to centrally manage the systems.**

Answer: D

Explanation:

The customer is seeking centralized policy management to reduce human error while maintaining compliance with their contractual obligations to AWS and Azure. Here's the evaluation of each option:

- * Option A: Cloud NGFWs at both CSPs; provide the customer a license for a Panorama virtual appliance from their CSP's marketplace of choice to centrally manage the systems
- * Cloud NGFW is a fully managed Next-Generation Firewall service by Palo Alto Networks, offered in AWS and Azure marketplaces. It integrates natively with the CSP infrastructure, making it a good fit for customers with existing CSP agreements.
- * Panorama, Palo Alto Networks' centralized management solution, can be deployed as a virtual appliance in the CSP marketplace of choice, enabling centralized policy management across all NGFWs.
- * This option addresses the customer's need for centralized management while leveraging their existing contracts with AWS and Azure.
- * This option is appropriate.
- * Option B: Cloud NGFWs in AWS and VM-Series firewall in Azure; the customer selects a PAYG licensing Panorama deployment in their CSP of choice
- * This option suggests using Cloud NGFW in AWS but VM-Series firewalls in Azure. While VM-Series is a flexible virtual firewall solution, it may not align with the customer's stated preference for CSP-managed services like Cloud NGFW.
- * This option introduces a mix of solutions that could complicate centralized management and reduce operational efficiency.
- * This option is less appropriate.
- * Option C: VM-Series firewalls in both CSPs; manually built Panorama in the CSP of choice on a host of either type: Palo Alto Networks provides a license
- * VM-Series firewalls are well-suited for cloud deployments but require more manual configuration compared to Cloud NGFW.
- * Building a Panorama instance manually on a host increases operational overhead and does not leverage the customer's existing CSP marketplaces.
- * This option is less aligned with the customer's needs.
- * Option D: VM-Series firewall and CN-Series firewall in both CSPs; provide the customer a private-offer Panorama virtual appliance from their CSP's marketplace of choice to centrally manage the systems
- * This option introduces both VM-Series and CN-Series firewalls in both CSPs. While CN-Series firewalls are designed for Kubernetes environments, they may not be relevant if the customer does not specifically require container-level security.
- * Adding CN-Series firewalls may introduce unnecessary complexity and costs.
- * This option is not appropriate.

References:

- * Palo Alto Networks documentation on Cloud NGFW
- * Panorama overview in Palo Alto Knowledge Base
- * VM-Series firewalls deployment guide in CSPs: Palo Alto Documentation

NEW QUESTION # 36

While responding to a customer RFP, a systems engineer (SE) is presented the question, "How do PANW firewalls enable the mapping of transactions as part of Zero Trust principles?" Which two narratives can the SE use to respond to the question? (Choose two.)

- A. Emphasize Zero Trust as an ideology, and that the customer decides how to align to Zero Trust principles.
- **B. Describe how Palo Alto Networks NGFW Security policies are built by using users, applications, and data objects.**
- C. Reinforce the importance of decryption and security protections to verify traffic that is not malicious.
- **D. Explain how the NGFW can be placed in the network so it has visibility into every traffic flow.**

Answer: B,D

Explanation:

Zero Trust is a strategic framework for securing infrastructure and data by eliminating implicit trust and continuously validating every stage of digital interaction. Palo Alto Networks NGFWs are designed with native capabilities to align with Zero Trust principles, such as monitoring transactions, validating identities, and enforcing least-privilege access. The following narratives effectively address

the customer's question:

* Option A: While emphasizing Zero Trust as an ideology is accurate, this response does not directly explain how Palo Alto Networks firewalls facilitate mapping of transactions. It provides context but is insufficient for addressing the technical aspect of the question.

* Option B: Decryption and security protections are important for identifying malicious traffic, but they are not specific to mapping transactions within a Zero Trust framework. This response focuses on a subset of security functions rather than the broader concept of visibility and policy enforcement.

* Option C (Correct): Placing the NGFW in the network provides visibility into every traffic flow across users, devices, and applications. This allows the firewall to map transactions and enforce Zero Trust principles such as segmenting networks, inspecting all traffic, and controlling access. With features like App-ID, User-ID, and Content-ID, the firewall provides granular insights into traffic flows, making it easier to identify and secure transactions.

* Option D (Correct): Palo Alto Networks NGFWs use security policies based on users, applications, and data objects to align with Zero Trust principles. Instead of relying on IP addresses or ports, policies are enforced based on the application's behavior, the identity of the user, and the sensitivity of the data involved. This mapping ensures that only authorized users can access specific resources, which is a cornerstone of Zero Trust.

References:

* Zero Trust Framework: <https://www.paloaltonetworks.com/solutions/zero-trust>

* Security Policy Best Practices for Zero Trust: <https://docs.paloaltonetworks.com>

NEW QUESTION # 37

Regarding APIs, a customer RFP states: "The vendor's firewall solution must provide an API with an enforcement mechanism to deactivate API keys after two hours." How should the response address this clause?

- A. No - The API keys can be made, but there is no method to deactivate them based on time.
- B. No - The PAN-OS XML API does not support keys.
- C. Yes - The default setting must be changed from no limit to 120 minutes.
- D. Yes - This is the default setting for API keys.

Answer: C

Explanation:

Palo Alto Networks' PAN-OS supports API keys for authentication when interacting with the firewall's RESTful and XML-based APIs. By default, API keys do not have an expiration time set, but the expiration time for API keys can be configured by an administrator to meet specific requirements, such as a time-based deactivation after two hours. This is particularly useful for compliance and security purposes, where API keys should not remain active indefinitely.

Here's an evaluation of the options:

* Option A: This is incorrect because the default setting for API keys does not include an expiration time. By default, API keys are valid indefinitely unless explicitly configured otherwise.

* Option B: This is incorrect because PAN-OS fully supports API keys. The API keys are integral to managing access to the firewall's APIs and provide a secure method for authentication.

* Option C: This is incorrect because PAN-OS does support API key expiration when explicitly configured. While the default is "no expiration," the feature to configure an expiration time (e.g., 2 hours) is available.

* Option D (Correct): The correct response to the RFP clause is that the default API key settings need to be modified to set the expiration time to 120 minutes (2 hours). This aligns with the customer requirement to enforce API key deactivation based on time. Administrators can configure this using the PAN-OS management interface or the CLI.

How to Configure API Key Expiration (Steps):

* Access the Web Interface or CLI on the firewall.

* Navigate to Device > Management > API Key Lifetime Settings (on the GUI).

* Set the desired expiration time (e.g., 120 minutes).

* Alternatively, use the CLI to configure the API key expiration:

```
set deviceconfig system api-key-expiry <time-in-minutes>
```

```
commit
```

* Verify the configuration using the show command or by testing API calls to ensure the key expires after the set duration.

References:

Palo Alto Networks API Documentation: <https://docs.paloaltonetworks.com/apis> Configuration Guide: Managing API Key Expiration

NEW QUESTION # 38

Which statement applies to the default configuration of a Palo Alto Networks NGFW?

- A. The default policy action allows all traffic unless explicitly denied.
- B. Security profiles are applied to all policies by default, eliminating implicit trust of any data traversing the firewall.
- **C. The default policy action for interzone traffic is deny, eliminating implicit trust between security zones.**
- D. The default policy action for intrazone traffic is deny, eliminating implicit trust within a security zone.

Answer: C

Explanation:

The default configuration of a Palo Alto Networks NGFW includes a set of default security rules that determine how traffic is handled when no explicit rules are defined. Here's the explanation for each option:

* Option A: Security profiles are applied to all policies by default, eliminating implicit trust of any data traversing the firewall

* Security profiles (such as Antivirus, Anti-Spyware, and URL Filtering) are not applied to any policies by default. Administrators must explicitly apply them to security rules.

* This statement is incorrect.

* Option B: The default policy action for intrazone traffic is deny, eliminating implicit trust within a security zone

* By default, traffic within the same zone (intrazone traffic) is allowed. For example, traffic between devices in the "trust" zone is permitted unless explicitly denied by an administrator.

* This statement is incorrect.

* Option C: The default policy action allows all traffic unless explicitly denied

* Palo Alto Networks firewalls do not have an "allow all" default rule. Instead, they include a default "deny all" rule for interzone traffic and an implicit "allow" rule for intrazone traffic.

* This statement is incorrect.

* Option D: The default policy action for interzone traffic is deny, eliminating implicit trust between security zones

* By default, traffic between different zones (interzone traffic) is denied. This aligns with the principle of zero trust, ensuring that no traffic is implicitly allowed between zones.

Administrators must define explicit rules to allow interzone traffic.

* This statement is correct.

References:

* Palo Alto Networks documentation on Security Policy Defaults

* Knowledge Base article on Default Security Rules

NEW QUESTION # 39

.....

Our PSE-Strata-Pro-24 training engine is revised by experts and approved by experienced professionals, which simplify complex concepts and add examples, simulations to explain anything that may be difficult to understand. Therefore, using PSE-Strata-Pro-24 Exam Prep makes it easier for learners to grasp and simplify the content of important PSE-Strata-Pro-24 information, no matter novice or experienced, which can help you save a lot of time and energy eventually.

PSE-Strata-Pro-24 Official Cert Guide: <https://www.testbraindump.com/PSE-Strata-Pro-24-exam-prep.html>

- Reliable PSE-Strata-Pro-24 Guide Files PSE-Strata-Pro-24 Reliable Exam Vce Test PSE-Strata-Pro-24 Pattern
 Search for ⇒ PSE-Strata-Pro-24 ⇐ and obtain a free download on [www.torrentvalid.com] Valid Dumps PSE-Strata-Pro-24 Book
- 2025 High-quality Reliable PSE-Strata-Pro-24 Exam Registration | 100% Free PSE-Strata-Pro-24 Official Cert Guide
Search for « PSE-Strata-Pro-24 » and download it for free immediately on ➡ www.pdfvce.com Original PSE-Strata-Pro-24 Questions
- Excellent 100% Free PSE-Strata-Pro-24 – 100% Free Reliable Exam Registration | PSE-Strata-Pro-24 Official Cert Guide
 Search for ▷ PSE-Strata-Pro-24 ◁ on ➡ www.lead1pass.com immediately to obtain a free download PSE-Strata-Pro-24 Valid Test Pass4sure
- Original PSE-Strata-Pro-24 Questions PSE-Strata-Pro-24 Valid Exam Answers ⇐ Test PSE-Strata-Pro-24 Cram
Open “ www.pdfvce.com ” enter ► PSE-Strata-Pro-24 and obtain a free download Test PSE-Strata-Pro-24 Pattern
- Reliable PSE-Strata-Pro-24 Exam Registration - 100% Pass Palo Alto Networks PSE-Strata-Pro-24 First-grade Official Cert Guide
The page for free download of [PSE-Strata-Pro-24] on ➡ www.examsreviews.com will open immediately Dumps PSE-Strata-Pro-24 Collection
- Pass Guaranteed Quiz Palo Alto Networks - Reliable PSE-Strata-Pro-24 Exam Registration Open www.pdfvce.com
 and search for [PSE-Strata-Pro-24] to download exam materials for free Pass PSE-Strata-Pro-24 Rate
- Palo Alto Networks Reliable PSE-Strata-Pro-24 Exam Registration: Palo Alto Networks Systems Engineer Professional -

