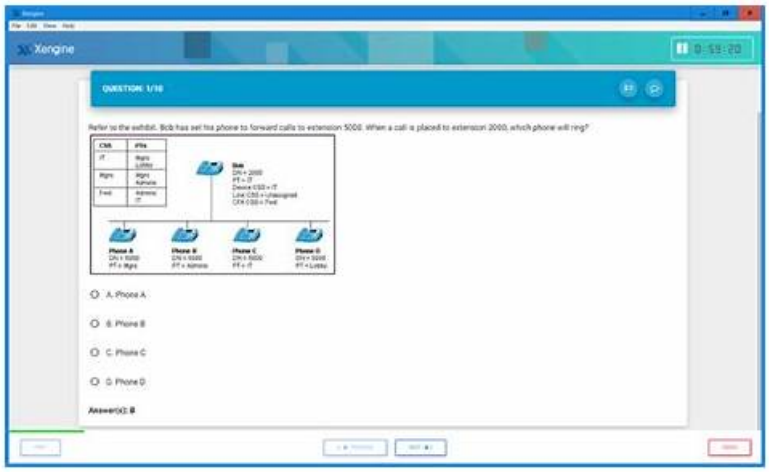
Amazing PSE-Strata-Pro-24 Exam Simulation: Palo Alto Networks Systems Engineer Professional - Hardware Firewall give you the latest Practice Dumps - ITdumpsfree



2026 Latest ITdumpsfree PSE-Strata-Pro-24 PDF Dumps and PSE-Strata-Pro-24 Exam Engine Free Share: https://drive.google.com/open?id=1sS1o4hx3HjcidzbbDBJQmw0gCy04div

Palo Alto Networks certification can improve companies' competition, enlarge companies' business products line and boost IT staff constant learning. Many companies may choose PSE-Strata-Pro-24 valid exam study guide for staff while they are urgent to need one engineer with a useful certification so that they can get orders from this Palo Alto Networks or get the management agency right. Our PSE-Strata-Pro-24 valid exam study guide will be the best valid choice for them.

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

Topic	Details
Topic 1	• 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 2	• 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	• Network Security Strategy and Best Practices: This section of the exam measures the skills of Security Strategy Specialists and highlights the importance of the Palo Alto Networks five-step Zero Trust methodology. Candidates must understand how to approach and apply the Zero Trust model effectively while emphasizing best practices to ensure robust network security.
Topic 4	• 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 Reliable Test Cost <<

New Palo Alto Networks PSE-Strata-Pro-24 Dumps Free, Premium PSE-Strata-Pro-24 Exam

PSE-Strata-Pro-24 test guide is an examination material written by many industry experts based on the examination outlines of the calendar year and industry development trends. Its main purpose is to help students who want to obtain the certification of PSE-Strata-Pro-24 to successfully pass the exam. Compared with other materials available on the market, the main feature of PSE-Strata-Pro-24 exam materials doesn't like other materials simply list knowledge points. It allows students to find time-saving and efficient learning methods while memorizing knowledge points. With PSE-Strata-Pro-24 study braindumps, learning from day and night will never happen. You can learn more with less time. You will become a master of learning in the eyes of others. With PSE-Strata-Pro-24 study braindumps, successfully passing the exam will no longer be a dream.

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q31-Q36):

NEW QUESTION # 31
Which three use cases are specific to Policy Optimizer? (Choose three.)

- A. Automating the tagging of rules based on historical log data
- B. Enabling migration from port-based rules to application-based rules
- C. Discovering 5-tuple attributes that can be simplified to 4-tuple attributes
- D. Discovering applications on the network and transitions to application-based policy over time
- E. Converting broad rules based on application filters into narrow rules based on application groups

Answer: A,B,D

Explanation:
The question asks for three use cases specific to Policy Optimizer, a feature in PAN-OS designed to enhance security policy management on Palo Alto Networks Strata Hardware Firewalls. Policy Optimizer helps administrators refine firewall rules by leveraging App-ID technology, transitioning from legacy port-based policies to application-based policies, and optimizing rule efficiency. Below is a detailed explanation of why options A, C, and E are the correct use cases, verified against official Palo Alto Networks documentation.
Step 1: Understanding Policy Optimizer in PAN-OS
Policy Optimizer is a tool introduced in PAN-OS 9.0 and enhanced in subsequent versions (e.g., 11.1), accessible under Policies > Policy Optimizer in the web interface. It analyzes traffic logs to:
* Identify applications traversing the network.
* Suggest refinements to security rules (e.g., replacing ports with App-IDs).
* Provide insights into rule usage and optimization opportunities.
Its primary goal is to align policies with Palo Alto Networks' application-centric approach, improving security and manageability on Strata NGFWs.

NEW QUESTION # 32
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. Reinforce the importance of decryption and security protections to verify traffic that is not malicious.
- B. Emphasize Zero Trust as an ideology, and that the customer decides how to align to Zero Trust principles.
- C. Explain how the NGFW can be placed in the network so it has visibility into every traffic flow.
- D. Describe how Palo Alto Networks NGFW Security policies are built by using users, applications, and data objects.

Answer: C,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 providesvisibility into every traffic flowacross 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 usesecurity policies based on users, applications, and data objectsto 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 # 33
The efforts of a systems engineer (SE) with an industrial mining company account have yielded interest in Palo Alto Networks as part of its effort to incorporate innovative design into operations using robots and remote-controlled vehicles in dangerous situations. A discovery call confirms that the company will receive control signals to its machines over a private mobile network using radio towers that connect to cloud-based applications that run the control programs.
Which two sets of solutions should the SE recommend?

- A. That IoT Security be included for visibility into the machines and to ensure that other devices connected to the network are identified and given risk and behavior profiles.
- B. That an Advanced CDSS bundle (Advanced Threat Prevention, Advanced WildFire, and Advanced URL Filtering) be procured to ensure the design receives advanced protection.
- C. That Cloud NGFW be included to protect the cloud-based applications from external access into the cloud service provider hosting them.
- D. That 5G Security be enabled and architected to ensure the cloud computing is not compromised in the commands it is sending to the onsite machines.

Answer: A,D

Explanation:
* 5G Security (Answer A):
* In this scenario, the mining company operates on a private mobile network, likely powered by5G technologyto ensure low latency and high bandwidth for controlling robots and vehicles.
* Palo Alto Networks5G Securityis specifically designed to protect private mobile networks. It prevents exploitation of vulnerabilities in the 5G infrastructure and ensures the control signals sent to the machines arenot compromisedby attackers.
* Key features include network slicing protection, signaling plane security, and secure user plane communications.
* IoT Security (Answer C):
* The mining operation depends on machines and remote-controlled vehicles, which are IoT devices.
* Palo Alto NetworksIoT Securityprovides:
* Full device visibilityto detect all IoT devices (such as robots, remote vehicles, or sensors).
* Behavioral analysisto create risk profiles and identify anomalies in the machines' operations.
* This ensures a secure environment for IoT devices, reducing the risk of a device being exploited.
* Why Not Cloud NGFW (Answer B):
* WhileCloud NGFWis critical for protecting cloud-based applications, the specific concern here is protecting control signals and IoT devicesrather than external access into the cloud service.
* The private mobile network and IoT device protection requirements make5G SecurityandIoT Securitymore relevant.
* Why Not Advanced CDSS Bundle (Answer D):
* The Advanced CDSS bundle (Advanced Threat Prevention, Advanced WildFire, Advanced URL Filtering) is essential for securing web traffic and detecting threats, but it does not address the specific challenges of securing private mobile networksandIoT devices.
* While these services can supplement the design, they are not theprimary focusin this use case.
References from Palo Alto Networks Documentation:

* 5G Security for Private Mobile Networks
* IoT Security Solution Brief
* Cloud NGFW Overview

NEW QUESTION # 34
Which two files are used to deploy CN-Series firewalls in Kubernetes clusters? (Choose two.)

- A. PAN-CN-NGFW-CONFIG
- B. PAN-CNI-MULTUS
- C. PAN-CN-MGMT-CONFIGMAP
- D. PAN-CN-MGMT

Answer: C,D

Explanation:
The CN-Series firewalls are Palo Alto Networks' containerized Next-Generation Firewalls (NGFWs) designed to secure Kubernetes clusters. Unlike the Strata Hardware Firewalls (e.g., PA-Series), which are physical appliances, the CN-Series is a software-based solution deployed within containerized environments.
The question focuses on the specific files used to deploy CN-Series firewalls in Kubernetes clusters. Based on Palo Alto Networks' official documentation, the two correct files are PAN-CN-MGMT-CONFIGMAP and PAN-CN-MGMT. Below is a detailed explanation of why these files are essential, with references to CN- Series deployment processes (noting that Strata hardware documentation is not directly applicable here but is contextualized for clarity).
Step 1: Understanding CN-Series Deployment in Kubernetes
The CN-Series firewall consists of two primary components: the CN-MGMT (management plane) and the CN-NGFW (data plane). These components are deployed as containers in a Kubernetes cluster, orchestrated using YAML configuration files. The deployment process involves defining resources such as ConfigMaps, Pods, and Services to instantiate and manage the CN-Series components. The files listed in the question are Kubernetes manifests or configuration files used during this process.
* CN-MGMT Role:The CN-MGMT container handles the management plane, providing configuration, logging, and policy enforcement for the CN-Series firewall. It requires a dedicated YAML file to define its deployment.
* CN-NGFW Role:The CN-NGFW container handles the data plane, inspecting traffic within the Kubernetes cluster. It relies on configurations provided by CN-MGMT and additional networking setup (e.g., via CNI plugins).
* ConfigMaps:Kubernetes ConfigMaps store configuration data separately from container images, making them critical for passing settings to CN-Series components.

NEW QUESTION # 35
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. Yes - This is the default setting for API keys.
- B. Yes - The default setting must be changed from no limit to 120 minutes.
- C. No - The API keys can be made, but there is no method to deactivate them based on time.
- D. No - The PAN-OS XML API does not support keys.

Answer: B

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 # 36
.....