Pass Guaranteed Palo Alto Networks PSE-Strata-Pro-24 - First-grade Exam Palo Alto Networks Systems Engineer Professional - Hardware Firewall Review

What's more, part of that Lead2PassExam PSE-Strata-Pro-24 dumps now are free: https://drive.google.com/open?id=19kCFlKrpAAPejqxsaa5eMGMskJSTD_Pm

These Palo Alto Networks PSE-Strata-Pro-24 questions will give you an accurate foresight of the Palo Alto Networks PSE-Strata-Pro-24 examination format. This Palo Alto Networks PSE-Strata-Pro-24 is easily downloadable and even printable, this way you can also pursue paper study if that is your preferred method. The portability of this material makes it handier since you can access it on any smart device such as smart phones, laptops, tablets, etc. These Palo Alto Networks PSE-Strata-Pro-24 features make this prep method the most comfortable one.

In addition to the environment, we also provide simulations of papers. You really have to believe in the simulation paper of our PSE-Strata-Pro-24 study materials. With our PSE-Strata-Pro-24 practice engine, you can know that practicing the questions and answers are a enjoyable experience and it is an interactive system. If you are answering the questions rightly, then the result will show right, and if you choose the wrong answer, then it will show wrong. And when you finish the PSE-Strata-Pro-24 Exam Questions, the scores will come up as well.

>> Exam PSE-Strata-Pro-24 Review <<

Reliable PSE-Strata-Pro-24 Exam Practice | PSE-Strata-Pro-24 Reliable Test Online

We know that the standard for most workers become higher and higher; so we also set higher goal on our PSE-Strata-Pro-24 guide questions. Our training materials put customers' interests in front of other points, committing us to the advanced PSE-Strata-Pro-24 learning materials all along. Until now, we have simplified the most complicated PSE-Strata-Pro-24 Guide questions and designed a straightforward operation system, with the natural and seamless user interfaces of PSE-Strata-Pro-24 exam question grown to be more fluent, we assure that our practice materials provide you a total ease of use.

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

Topic	Details
Topic 1	• 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 2	• 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 3	• 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 4	• 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.

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

NEW QUESTION # 31
Which three tools can a prospective customer use to evaluate Palo Alto Networks products to assess where they will fit in the existing architecture? (Choose three)

- A. Expedition
- B. Policy Optimizer
- C. Ultimate Test Drive
- D. Proof of Concept (POC)
- E. Security Lifecycle Review (SLR)

Answer: C,D,E

Explanation:
When evaluating Palo Alto Networks products, prospective customers need tools that can help them assess compatibility, performance, and value within their existing architecture. The following tools are the most relevant:
* Why "Proof of Concept (POC)" (Correct Answer A)?A Proof of Concept is a hands-on evaluation that allows the customer to deploy and test Palo Alto Networks products directly within their environment. This enables them to assess real-world performance, compatibility, and operational impact.
* Why "Security Lifecycle Review (SLR)" (Correct Answer C)?An SLR provides a detailed report of a customer's network security posture based on data collected during a short evaluation period. It highlights risks, vulnerabilities, and active threats in the customer's network, demonstrating how Palo Alto Networks solutions can address those risks. SLR is a powerful tool for justifying the value of a product in the customer's architecture.
* Why "Ultimate Test Drive" (Correct Answer D)?The Ultimate Test Drive is a guided hands-on workshop provided by Palo Alto Networks that allows prospective customers to explore product features and capabilities in a controlled environment. It is ideal for customers who want to evaluate products without deploying them in their production network.
* Why not "Policy Optimizer" (Option B)?Policy Optimizer is used after a product has been deployed to refine security policies by identifying unused or overly permissive rules. It is not designed for pre- deployment evaluations.
* Why not "Expedition" (Option E)?Expedition is a migration tool that assists with the conversion of configurations from third-party firewalls or existing Palo Alto Networks firewalls. It is not a tool for evaluating the suitability of products in the customer's architecture.
Reference: Palo Alto Networks SLR documentation and Ultimate Test Drive overview confirm these tools' roles in product evaluation.

NEW QUESTION # 32
A prospective customer has provided specific requirements for an upcoming firewall purchase, including the need to process a

minimum of 200,000 connections per second while maintaining at least 15 Gbps of throughput with App-ID and Threat Prevention enabled.
What should a systems engineer do to determine the most suitable firewall for the customer?

- A. Download the firewall sizing tool from the Palo Alto Networks support portal.
- B. Use the online product configurator tool provided on the Palo Alto Networks website.
- C. Use the product selector tool available on the Palo Alto Networks website.
- D. Upload 30 days of customer firewall traffic logs to the firewall calculator tool on the Palo Alto Networks support portal.

Answer: D

Explanation:
The prospective customer has provided precise performance requirements for their firewall purchase, and the systems engineer must recommend a suitable Palo Alto Networks Strata Hardware Firewall (e.
g., PA-Series) model. The requirements include a minimum of 200,000 connections per second (CPS) and 15 Gbps of throughput with App-ID and Threat Prevention enabled. Let's evaluate the best approach to meet these needs.
Step 1: Understand the Requirements
* Connections per Second (CPS): 200,000 new sessions per second, indicating the firewall's ability to handle high transaction rates (e.g., web traffic, API calls).
* Throughput with App-ID and Threat Prevention: 15 Gbps, measured with application identification and threat prevention features active, reflecting real-world NGFW performance.
* Goal: Identify a PA-Series model that meets or exceeds these specs while considering the customer's actual traffic profile for optimal sizing.

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 an Advanced CDSS bundle (Advanced Threat Prevention, Advanced WildFire, and Advanced URL Filtering) be procured to ensure the design receives advanced protection.
- B. That Cloud NGFW be included to protect the cloud-based applications from external access into the cloud service provider hosting them.
- C. 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.
- D. 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.

Answer: C,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 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. SSL decryption traffic amounts vary from network to network.
- C. Large average transaction sizes consume more processing power to decrypt.
- D. 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.

Answer: A,B

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 directlyrelevant to sizing considerations for firewall deployments with decryption enabled.

NEW QUESTION # 35
Which two files are used to deploy CN-Series firewalls in Kubernetes clusters? (Choose two.)

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

Answer: B,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.
Reference:
"CN-Series Deployment Guide" (Palo Alto Networks) outlines the deployment process, stating, "The CN- Series firewall is deployed using Kubernetes YAML files that define the management and data plane components." Step 2: Identifying the Correct Files Option B: PAN-CN-MGMT-CONFIGMAP Explanation:The PAN-CN-MGMT-CONFIGMAP file is a Kubernetes ConfigMap used to store configuration data for the CN-MGMT component. This file includes settings such as Panorama IP addresses, authentication keys, and other parameters needed to initialize the CN-Series management plane. It is applied to the cluster before deploying the CN-MGMT Pod to ensure the management plane has the necessary configuration.
Purpose: Provides the CN-MGMT container with external configuration details, such as connectivity to Panorama for centralized management.
Deployment Step: The ConfigMap is created using a command like kubectl apply -f pan-cn-mgmt- configmap.yaml, as specified in the CN-Series setup process.
Strata Context: While Strata Hardware Firewalls (e.g., PA-400 Series) use Panorama for management too, the CN-Series adapts this concept to Kubernetes with ConfigMaps, a container-native construct.
Reference:
"Deploy the CN-Series Firewall" (Palo Alto Networks) specifies, "Create a ConfigMap using the pan-cn- mgmt-configmap.yaml file to provide configuration data for the CN-MGMT Pod."
"CN-Series Configuration Guide" confirms its role in passing Panorama settings to CN-MGMT.
Why Option B is Correct:PAN-CN-MGMT-CONFIGMAP is a mandatory file for deploying the CN-Series management plane, making it one of the two key files required.
Option C: PAN-CN-MGMT
Explanation:The PAN-CN-MGMT file is the YAML manifest that defines the CN-MGMT Pod deployment in the Kubernetes cluster. This file specifies the container image, resource requirements (e.g., CPU, memory), and references the PAN-CN-MGMT-CONFIGMAP for configuration data. It instantiates the management plane, enabling policy management and integration with Panorama.
Purpose: Deploys the CN-MGMT container as a Pod, which serves as the brain of the CN-Series firewall, managing policies and monitoring the data plane.
Deployment Step: Applied using kubectl apply -f pan-cn-mgmt.yaml, this file brings the management plane online after the ConfigMap is in place.
Strata Context: Unlike Strata hardware, which is pre-installed and configured physically, CN-MGMT uses Kubernetes orchestration, but its management function aligns with the PA-Series' management plane.
Reference:
"CN-Series Deployment Guide" states, "Use the pan-cn-mgmt.yaml file to deploy the CN-MGMT Pod, which manages the CN-Series firewall in the Kubernetes cluster."
"CN-Series Tech Docs" detail the YAML structure for CN-MGMT, including its dependence on the ConfigMap.
Why Option C is Correct:PAN-CN-MGMT is the core deployment file for the CN-Series management plane, making it essential for Kubernetes deployment.
Why Other Options Are Incorrect
Option A: PAN-CN-NGFW-CONFIG
Analysis:There is no file named PAN-CN-NGFW-CONFIG in Palo Alto Networks' CN-Series deployment documentation. The CN-NGFW (data plane) component uses a separate YAML file, typically named pan-cn- ngfw.yaml, to deploy its Pods. However, no "CONFIG" suffix exists, and the data plane deployment relies on CN-MGMT for configuration rather than a standalone ConfigMap with this name.
Reference: "Deploy the CN-Series Firewall" mentions pan-cn-ngfw.yaml for the data plane, not PAN-CN- NGFW-CONFIG.
Option D: PAN-CNI-MULTUS
Analysis:The PAN-CNI-MULTUS file relates to the Container Network Interface (CNI) plugin used for advanced networking in CN-Series deployments, such as Multus for multiple network interfaces. While it is part of the networking setup (e.g., to enable traffic redirection to CN-NGFW), it is not one of the primary files for deploying the CN-Series firewall itself. The question asks for files directly tied to firewall deployment, not optional networking enhancements.
Reference: "CN-Series Networking Guide" mentions Multus CNI as an optional configuration, applied separately via pan-cni-

multus.yaml, not a core deployment file.
Conclusion
The CN-Series firewall deployment in Kubernetes clusters relies on PAN-CN-MGMT-CONFIGMAP (B) to provide configuration data and PAN-CN-MGMT (C) to deploy the management plane Pod. These two files are explicitly required per Palo Alto Networks' CN-Series documentation, ensuring the firewall's management component is operational. While Strata Hardware Firewalls like the PA-Series operate in physical environments, the CN-Series adapts similar NGFW capabilities to containers, with these files serving as the Kubernetes equivalent of hardware setup and configuration.

NEW QUESTION # 36
.....

Sometimes if you want to pass an important test, to try your best to exercise more questions is very necessary, which will be met by our PSE-Strata-Pro-24 exam software, and the professional answer analysis also can help you have a better understanding. the multiple versions of free demo of PSE-Strata-Pro-24 Exam Materials can be offered in our website. Try to find which version is most to your taste; we believe that our joint efforts can make you pass PSE-Strata-Pro-24 certification exam.

P.S. Free & New PSE-Strata-Pro-24 dumps are available on Google Drive shared by Lead2PassExam: https://drive.google.com/open?id=19kCFlKrpAAPejqxsaa5eMGMskJSTD_Pm