Official PSE-Strata-Pro-24 Study Guide - Test PSE-Strata-Pro-24 Pass4sure

DOWNLOAD the newest TestKingIT PSE-Strata-Pro-24 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=16-w8iG5XL9lo35ZMB_CaBUlZTVQ7dw7K

Many exam candidates attach great credence to our PSE-Strata-Pro-24 simulating exam. You can just look at the hot hit on our website on the PSE-Strata-Pro-24 practice engine, and you will be surprised to find it is very popular and so many warm feedbacks are written by our loyal customers as well. Our PSE-Strata-Pro-24 study prep does not need any ads, their quality has propaganda effect themselves. As a result, the pass rate of our PSE-Strata-Pro-24 exam braindumps is high as 98% to 100%.

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

Topic	Details
Topic 1	• 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	• 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 3	• 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	• 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.

>> Official PSE-Strata-Pro-24 Study Guide <<

Test PSE-Strata-Pro-24 Pass4sure | Real PSE-Strata-Pro-24 Exam Dumps

TestKingIT is a website that not the same as other competitor, because it provide all candidates with valuable PSE-Strata-Pro-24 exam questions, aiming to help them who meet difficult in pass the PSE-Strata-Pro-24 exam. Not only does it not provide poor quality PSE-Strata-Pro-24 Exam Materials like some websites, it does not have the same high price as some websites. If you would like to try PSE-Strata-Pro-24 learning braindumps from our website, it must be the most effective investment for your money.

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q49-Q54):

NEW QUESTION # 49
A customer asks a systems engineer (SE) how Palo Alto Networks can claim it does not lose throughput performance as more Cloud-Delivered Security Services (CDSS) subscriptions are enabled on the firewall.
Which two concepts should the SE explain to address the customer's concern? (Choose two.)

- A. Parallel Processing
- B. Management Data Plane Separation
- C. Advanced Routing Engine
- D. Single Pass Architecture

Answer: A,D

Explanation:
The customer's question focuses on how Palo Alto Networks Strata Hardware Firewalls maintain throughput performance as more Cloud-Delivered Security Services (CDSS) subscriptions-such as Threat Prevention, URL Filtering, WildFire, DNS Security, and others-are enabled. Unlike traditional firewalls where enabling additional security features often degrades performance, Palo Alto Networks leverages its unique architecture to minimize this impact. The systems engineer (SE) should explain two key concepts-Parallel Processing andSingle Pass Architecture-which are foundational to the firewall's ability to sustain throughput. Below is a detailed explanation, verified against Palo Alto Networks documentation.
Step 1: Understanding Cloud-Delivered Security Services (CDSS) and Performance Concerns CDSS subscriptions enhance the Strata Hardware Firewall's capabilities by integrating cloud-based threat intelligence and advanced security features into PAN-OS. Examples include:
* Threat Prevention: Blocks exploits, malware, and command-and-control traffic.
* WildFire: Analyzes unknown files in the cloud for malware detection.
* URL Filtering: Categorizes and controls web traffic.
Traditionally, enabling such services on other firewalls increases processing overhead, as each feature requires separate packet scans or additional hardware resources, leading to latency and throughput loss. Palo Alto Networks claims consistent performance due to its innovative design, rooted in theSingle Pass Parallel Processing (SP3)architecture.

NEW QUESTION # 50
In addition to DNS Security, which three Cloud-Delivered Security Services (CDSS) subscriptions are minimum recommendations for all NGFWs that handle north-south traffic? (Choose three)

- A. Advanced Threat Prevention
- B. Advanced URL Filtering
- C. Enterprise DLP
- D. Advanced WildFire
- E. SaaS Security

Answer: A,B,D

Explanation:
North-south traffic refers to the flow of data in and out of a network, typically between internal resources and the internet. To secure this type of traffic, Palo Alto Networks recommends specific CDSS subscriptions in addition to DNS Security:

A: SaaS Security
SaaS Security is designed for monitoring and securing SaaS application usage but is not essential for handling typical north-south traffic.
B: Advanced WildFire
Advanced WildFire provides cloud-based malware analysis and sandboxing to detect and block zero-day threats. It is a critical component for securing north-south traffic against advanced malware.
C: Enterprise DLP
Enterprise DLP focuses on data loss prevention, primarily for protecting sensitive data. While important, it is not a minimum recommendation for securing north-south traffic.
D: Advanced Threat Prevention
Advanced Threat Prevention (ATP) replaces traditional IPS and provides inline detection and prevention of evasive threats in north-south traffic. It is a crucial recommendation for protecting against sophisticated threats.
E: Advanced URL Filtering
Advanced URL Filtering prevents access to malicious or harmful URLs. It complements DNS Security to provide comprehensive web protection for north-south traffic.
Key Takeaways:
* Advanced WildFire, Advanced Threat Prevention, and Advanced URL Filtering are minimum recommendations for NGFWs handling north-south traffic, alongside DNS Security.
* SaaS Security and Enterprise DLP, while valuable, are not minimum requirements for this use case.
References:
* Palo Alto Networks NGFW Best Practices
* Cloud-Delivered Security Services

NEW QUESTION # 51
Which three descriptions apply to a perimeter firewall? (Choose three.)

- A. Network layer protection for the outer edge of a network
- B. Securing east-west traffic in a virtualized data center with flexible resource allocation
- C. Guarding against external attacks
- D. Primarily securing north-south traffic entering and leaving the network
- E. Power utilization less than 500 watts sustained

Answer: A,C,D

Explanation:
Aperimeter firewallis traditionally deployed at the boundary of a network to protect it from external threats.
It provides a variety of protections, including blocking unauthorized access, inspecting traffic flows, and safeguarding sensitive resources. Here is how the options apply:
* Option A (Correct):Perimeter firewalls providenetwork layer protectionby filtering and inspecting traffic entering or leaving the network at the outer edge. This is one of their primary roles.
* Option B:Power utilization is not a functional or architectural aspect of a firewall and is irrelevant when describing the purpose of a perimeter firewall.
* Option C:Securing east-west traffic is more aligned withdata center firewalls, whichmonitor lateral (east-west) movement of traffic within a virtualized or segmented environment. A perimeter firewall focuses on north-south traffic instead.
* Option D (Correct):A perimeter firewall primarily securesnorth-south traffic, which refers to traffic entering and leaving the network. It ensures that inbound and outbound traffic adheres to security policies.
* Option E (Correct):Perimeter firewalls play a critical role inguarding against external attacks, such as DDoS attacks, malicious IP traffic, and other unauthorized access attempts.
References:
* Palo Alto Networks Firewall Deployment Use Cases: https://docs.paloaltonetworks.com
* Security Reference Architecture for North-South Traffic Control.

NEW QUESTION # 52
A company with Palo Alto Networks NGFWs protecting its physical data center servers is experiencing a performance issue on its Active Directory (AD) servers due to high numbers of requests and updates the NGFWs are placing on the servers. How can the NGFWs be enabled to efficiently identify users without overloading the AD servers?

- A. Configure an NGFW as a GlobalProtect gateway, then have all users run GlobalProtect agents to gather user information.

- B. Configure data redistribution to redistribute IP address-user mappings from a hub NGFW to the other spoke NGFWs.
- C. Configure an NGFW as a GlobalProtect gateway, then have all users run GlobalProtect Windows SSO to gather user information.
- D. Configure Cloud Identity Engine to learn the users' IP address-user mappings from the AD authentication logs.

Answer: D

Explanation:
When high traffic from Palo Alto Networks NGFWs to Active Directory servers causes performance issues, optimizing the way NGFWs gather user-to-IP mappings is critical. Palo Alto Networks offers multiple ways to collect user identity information, and Cloud Identity Engine provides a solution that reduces the load on AD servers while still ensuring efficient and accurate mapping.
* Option A (Correct): Cloud Identity Engine allows NGFWs to gather user-to-IP mappings directly from Active Directory authentication logs or other identity sources without placing heavy traffic on the AD servers. By leveraging this feature, the NGFW can offload authentication-related tasks and efficiently identify users without overloading AD servers. This solution is scalable and minimizes the overhead typically caused by frequent User-ID queries to AD servers.
* Option B: Using GlobalProtect Windows SSO to gather user information can add complexity and is not the most efficient solution for this problem. It requires all users to install GlobalProtect agents, which may not be feasible in all environments and can introduce operational challenges.
* Option C: Data redistribution involves redistributing user-to-IP mappings from one NGFW (hub) to other NGFWs (spokes). While this can reduce the number of queries sent to AD servers, it assumes the mappings are already being collected from AD servers by the hub, which means the performance issue on the AD servers would persist.
* Option D: Using GlobalProtect agents to gather user information is a valid method for environments where GlobalProtect is already deployed, but it is not the most efficient or straightforward solution for the given problem. It also introduces dependencies on agent deployment, configuration, and management.
How to Implement Cloud Identity Engine for User-ID Mapping:
* Enable Cloud Identity Engine from the Palo Alto Networks console.
* Integrate the Cloud Identity Engine with the AD servers to allow it to retrieve authentication logs directly.
* Configure the NGFWs to use the Cloud Identity Engine for User-ID mappings instead of querying the AD servers directly.
* Monitor performance to ensure the AD servers are no longer overloaded, and mappings are being retrieved efficiently.
References:
Cloud Identity Engine Overview: https://docs.paloaltonetworks.com/cloud-identity User-ID Best Practices: https://docs.paloaltonetworks.com

NEW QUESTION # 53
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. Describe how Palo Alto Networks NGFW Security policies are built by using users, applications, and data objects.
- B. Reinforce the importance of decryption and security protections to verify traffic that is not malicious.
- C. Emphasize Zero Trust as an ideology, and that the customer decides how to align to Zero Trust principles.
- D. Explain how the NGFW can be placed in the network so it has visibility into every traffic flow.

Answer: A,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 # 54
.....

Our PSE-Strata-Pro-24 PDF file is portable which means customers can carry this real questions document to any place. You just need smartphones, or laptops, to access this Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) PDF format. These Palo Alto Networks Systems Engineer Professional - Hardware Firewall (PSE-Strata-Pro-24) questions PDFs are also printable. So candidates who prefer to study in the old way which is paper study can print PSE-Strata-Pro-24 PDF questions as well.