

High Pass-Rate 100% Free PSE-Strata-Pro-24–100% Free Free Practice Exams | Exam PSE-Strata-Pro-24 Tutorial



What's more, part of that ExamsReviews PSE-Strata-Pro-24 dumps now are free: <https://drive.google.com/open?id=1GNHC5p-PvepLvOA1-yo7wE3eMR7-XAX1>

The efficiency of our PSE-Strata-Pro-24 study materials can be described in different aspects. PSE-Strata-Pro-24 practice guide is not only financially accessible, but time-saving and comprehensive to deal with the important questions trying to master them efficiently. You can obtain our PSE-Strata-Pro-24 Preparation engine within five minutes after you pay for it successfully and then you can study with it right away. Besides, if you have any question, our services will solve it at the first time.

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.

>> PSE-Strata-Pro-24 Free Practice Exams <<

PSE-Strata-Pro-24 Free Practice Exams - Palo Alto Networks Realistic Exam Palo Alto Networks Systems Engineer Professional - Hardware Firewall Tutorial

The talent is everywhere in modern society. This is doubly true for IT field. With the popularity of the computer, hardly anyone can't use a computer. Working in the IT industry, don't you feel pressure? Educational level is not representative of your strength. Education is just a ticket, however really keeping your status is your strength. As IT staff, how to cultivate your strength? It is a good choice to take IT certification test which can not only help you master more skills, also can get the certificate to prove your ability. Do you want to take Palo Alto Networks PSE-Strata-Pro-24 Exam that is very popular in recent?

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q16-Q21):

NEW QUESTION # 16

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 Cloud NGFW be included to protect the cloud-based applications from external access into the cloud service provider hosting them
- C. That an Advanced CDSS bundle (Advanced Threat Prevention, Advanced WildFire, and Advanced URL Filtering) be procured to ensure the design receives advanced protection.
- 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 by 5G technology to ensure low latency and high bandwidth for controlling robots and vehicles.

* Palo Alto Networks 5G Security is 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 are not compromised by 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 Networks IoT Security provides:

* Full device visibility to detect all IoT devices (such as robots, remote vehicles, or sensors).

* Behavioral analysis to 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):

* While Cloud NGFW is critical for protecting cloud-based applications, the specific concern here is protecting control signals and IoT devices rather than external access into the cloud service.

* The private mobile network and IoT device protection requirements make 5G Security and IoT Security more 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 networks and IoT devices.

* While these services can supplement the design, they are not the primary focus in this use case.

References from Palo Alto Networks Documentation:

* 5G Security for Private Mobile Networks

* IoT Security Solution Brief

* Cloud NGFW Overview

NEW QUESTION # 17

Which two compliance frameworks are included with the Premium version of Strata Cloud Manager (SCM)? (Choose two)

- A. National Institute of Standards and Technology (NIST)
- B. Health Insurance Portability and Accountability Act (HIPAA)
- C. Center for Internet Security (CIS)
- D. Payment Card Industry (PCI)

Answer: C,D

Explanation:

Strata Cloud Manager (SCM), part of Palo Alto Networks' Prisma Access and Prisma SD-WAN suite, provides enhanced visibility and control for managing compliance and security policies across the network. In the Premium version of SCM, compliance frameworks are pre-integrated to help organizations streamline audits and maintain adherence to critical standards.

A: Payment Card Industry (PCI)

PCI DSS (Data Security Standard) compliance is essential for businesses that handle payment card data. SCM Premium provides monitoring, reporting, and auditing tools that align with PCI requirements, ensuring that sensitive payment data is processed securely across the network.

B: National Institute of Standards and Technology (NIST)

NIST is a comprehensive cybersecurity framework used in various industries, especially in the government sector. However, NIST is not specifically included in SCM Premium; organizations may need separate configurations or external tools to fully comply with NIST guidelines.

C: Center for Internet Security (CIS)

CIS benchmarks provide security best practices for securing IT systems and data. SCM Premium includes CIS compliance checks, enabling organizations to maintain a strong baseline security posture and proactively address vulnerabilities.

D: Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a framework designed to protect sensitive healthcare information. While Palo Alto Networks provides general solutions that can be aligned with HIPAA compliance, it is not explicitly included as a compliance framework in SCM Premium.

Key Takeaways:

* The frameworks included in SCM Premium are PCI DSS and CIS.

* Other frameworks like NIST and HIPAA may require additional configurations or are supported indirectly but not explicitly part of the Premium compliance checks.

References:

* Palo Alto Networks Strata Cloud Manager Documentation

* Palo Alto Networks Compliance Resources

NEW QUESTION # 18

Which technique is an example of a DNS attack that Advanced DNS Security can detect and prevent?

- A. High entropy DNS domains
- B. DNS domain rebranding
- C. Polymorphic DNS
- D. CNAME cloaking

Answer: A

Explanation:

Advanced DNS Security on Palo Alto Networks firewalls is designed to identify and prevent a wide range of DNS-based attacks. Among the listed options, "High entropy DNS domains" is a specific example of a DNS attack that Advanced DNS Security can detect and block.

* Why "High entropy DNS domains" (Correct Answer A)? High entropy DNS domains are often used in attacks where randomly generated domain names (e.g., gfh34ksdu.com) are utilized by malware or bots to evade detection. This is a hallmark of Domain Generation Algorithms (DGA)-based attacks.

Palo Alto Networks firewalls with Advanced DNS Security use machine learning to detect such domains by analyzing the entropy (randomness) of DNS queries. High entropy values indicate the likelihood of a dynamically generated or malicious domain.

* Why not "Polymorphic DNS" (Option B)? While polymorphic DNS refers to techniques that dynamically change DNS records to avoid detection, it is not specifically identified as an attack type mitigated by Advanced DNS Security in Palo Alto Networks documentation. The firewall focuses more on the behavior of DNS queries, such as detecting DGA domains or anomalous DNS traffic patterns.

* Why not "CNAME cloaking" (Option C)? CNAME cloaking involves using CNAME records to redirect DNS queries to malicious or hidden domains. Although Palo Alto firewalls may detect and block malicious DNS redirections, the focus of Advanced DNS Security is primarily on identifying patterns of DNS abuse like DGA domains, tunneling, or high entropy queries.

* Why not "DNS domain rebranding" (Option D)? DNS domain rebranding involves changing the domain names associated with malicious activity to evade detection. This is typically a tactic used for persistence but is not an example of a DNS attack type specifically addressed by Advanced DNS Security.

Advanced DNS Security focuses on dynamic, real-time identification of suspicious DNS patterns, such as high entropy domains, DNS tunneling, or protocol violations. High entropy DNS domains are directly tied to attack mechanisms like DGAs, making this the correct answer.

NEW QUESTION # 19

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

Answer: A

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 # 20

A large global company plans to acquire 500 NGFWs to replace its legacy firewalls and has a specific requirement for centralized logging and reporting capabilities.

What should a systems engineer recommend?

- A. Highlight the efficiency of PAN-OS, which employs AI to automatically extract critical logs and generate daily executive reports, and confirm that the purchase of 500 NGFWs is sufficient.
- B. Deploy a pair of M-1000 log collectors in the customer data center, and route logs from all 500 firewalls to the log collectors for centralized logging and reporting.
- C. **Combine Panorama for firewall management with Palo Alto Networks' cloud-based Strata Logging Service to offer scalability for the company's logging and reporting infrastructure.**
- D. Use Panorama for firewall management and to transfer logs from the 500 firewalls directly to a third- party SIEM for centralized logging and reporting.

Answer: C

Explanation:

A large deployment of 500 firewalls requires a scalable, centralized logging and reporting infrastructure.

Here's the analysis of each option:

* Option A: Combine Panorama for firewall management with Palo Alto Networks' cloud-based Strata Logging Service to offer scalability for the company's logging and reporting infrastructure

* TheStrata Logging Service(or Cortex Data Lake) is a cloud-based solution that offers massive scalability for logging and reporting. Combined with Panorama, it allows for centralized log collection, analysis, and policy management without the need for extensive on-premises infrastructure.

* This approach is ideal for large-scale environments like the one described in the scenario, as it ensures cost-effectiveness and scalability.

* This is the correct recommendation.

* Option B: Use Panorama for firewall management and to transfer logs from the 500 firewalls directly to a third-party SIEM for centralized logging and reporting

* While third-party SIEM solutions can be integrated with Palo Alto Networks NGFWs, directly transferring logs from 500 firewalls to a SIEM can lead to bottlenecks and scalability issues.

Furthermore, relying on third-party solutions may not provide the same level of native integration as the Strata Logging Service.

* This is not the ideal recommendation.

* Option C: Highlight the efficiency of PAN-OS, which employs AI to automatically extract critical logs and generate daily executive reports, and confirm that the purchase of 500 NGFWs is sufficient

* While PAN-OS provides AI-driven insights and reporting, this option does not address the requirement for centralized logging and reporting. It also dismisses the need for additional infrastructure to handle logs from 500 firewalls.

* This is incorrect.

* Option D: Deploy a pair of M-1000 log collectors in the customer data center, and route logs from all 500 firewalls to the log collectors for centralized logging and reporting

* The M-1000 appliance is an on-premises log collector, but it has limitations in terms of scalability and storage capacity when compared to cloud-based options like the Strata Logging Service. Deploying only two M-1000 log collectors for 500 firewalls would result in potential performance and storage challenges.

* This is not the best recommendation.

References:

* Palo Alto Networks documentation on Panorama

* Strata Logging Service (Cortex Data Lake) overview in Palo Alto Networks Docs

NEW QUESTION # 21

.....

ExamsReviews expect to design such an efficient study plan to help you build a high efficient learning attitude for your further development. Our PSE-Strata-Pro-24 study torrent are cater every candidate no matter you are a student or office worker, a green hand or a staff member of many years' experience. Therefore, you have no need to worry about whether you can pass the PSE-Strata-Pro-24 Exam, because we guarantee you to succeed with our technology strength. The language of our PSE-Strata-Pro-24

exam questions are easy to follow and the pass rate of our PSE-Strata-Pro-24 learning guide is as high as 99% to 100%.

Exam PSE-Strata-Pro-24 Tutorial: <https://www.examsreviews.com/PSE-Strata-Pro-24-pass4sure-exam-review.html>

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

<https://drive.google.com/open?id=1GNHC5p-PvepLvOA1-yo7wE3eMR7-XAX1>