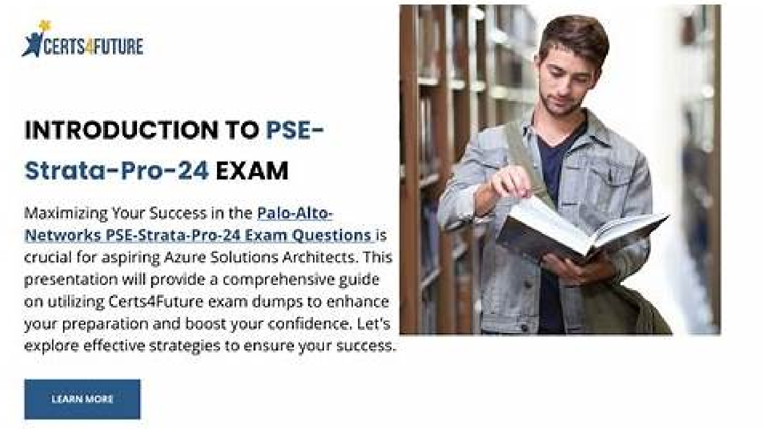
PSE-Strata-Pro-24 Valid Exam Fee - PSE-Strata-Pro-24 Exam Success



CERTS4FUTURE

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.

BONUS!!! Download part of BraindumpsPass PSE-Strata-Pro-24 dumps for free: https://drive.google.com/open?id=1fR-mYswQacRGOLDsk4LaXnOr2Z4XsqHt

Our PSE-Strata-Pro-24 exam questions just focus on what is important and help you achieve your goal. When the reviewing process gets some tense, our PSE-Strata-Pro-24 practice materials will solve your problems with efficiency. With high-quality PSE-Strata-Pro-24 Guide materials and flexible choices of learning mode, they would bring about the convenience and easiness for you. Every page is carefully arranged by our experts with clear layout and helpful knowledge to remember.

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	• 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	• 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	• 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.

>> PSE-Strata-Pro-24 Valid Exam Fee <<

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q40-Q45):

NEW QUESTION # 40
In addition to Advanced DNS Security, which three Cloud-Delivered Security Services (CDSS) subscriptions utilize inline machine learning (ML)? (Choose three)

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

Answer: A,B,C

NEW QUESTION # 41
Device-ID can be used in which three policies? (Choose three.)

- A. SD-WAN
- B. Security
- C. Policy-based forwarding (PBF)
- D. Decryption
- E. Quality of Service (QoS)

Answer: B,D,E

Explanation:
The question asks about the policies where Device-ID, a feature of Palo Alto Networks NGFWs, can be applied. Device-ID enables the firewall to identify and classify devices (e.g., IoT, endpoints) based on attributes like device type, OS, or behavior, enhancing policy enforcement. Let's evaluate its use across the specified policy types.
Step 1: Understand Device-ID
Device-ID leverages the IoT Security subscription and integrates with the Strata Firewall to provide device visibility and control. It uses data from sources like DHCP, HTTP headers, and machine learning to identify devices and allows policies to reference device objects (e.g., "IP Camera," "Medical Device"). This feature is available on PA-Series firewalls running PAN-OS 10.0 or later with the appropriate license.
Reference: PAN-OS Administrator's Guide - Device-ID (docs.paloaltonetworks.com/pan-os/10-2/pan-os- admin/policy/device-id).
Step 2: Define Policy Types
Palo Alto NGFWs support various policy types, each serving a distinct purpose:
Security: Controls traffic based on source, destination, application, user, and device.
Decryption: Manages SSL/TLS decryption based on traffic attributes.
Policy-Based Forwarding (PBF): Routes traffic based on predefined rules.
SD-WAN: Manages WAN traffic with performance-based routing (requires SD-WAN subscription).
Quality of Service (QoS): Prioritizes or limits bandwidth for traffic.
Device-ID's applicability depends on whether a policy type supports device objects as a match criterion.
Step 3: Evaluate Each Option
A). Security
Description: Security policies (Policies > Security) define allow/deny rules for traffic, using match criteria like source/destination IP, zones, users, applications, and devices.
Device-ID Integration: With Device-ID enabled, security policies can use device objects (e.g., "IP Camera") in the Source or Destination fields. This allows granular control, such as blocking untrusted IoT devices or allowing specific device types.
Example: A rule allowing only "Windows Laptops" to access a server.

Fit: Supported and a primary use case for Device-ID.
Reference: PAN-OS Device-ID in Security Policies (docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin /policy/use-device-id-in-a-security-policy).
B). Decryption
Description: Decryption policies (Policies > Decryption) determine which traffic to decrypt or bypass, based on source, destination, service, or URL category.
Device-ID Integration: Starting in PAN-OS 10.0, decryption policies support device objects as match criteria. This enables selective decryption based on device type (e.g., decrypt traffic from "IoT Sensors" but not "Corporate Laptops").
Example: Bypassing decryption for privacy-sensitive medical devices.
Fit: Supported and enhances decryption granularity.
Reference: PAN-OS Decryption with Device-ID (docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin /decryption/configure-decryption-policy#device-id).
C). Policy-Based Forwarding (PBF)
Description: PBF policies (Policies > Policy Based Forwarding) route traffic to specific interfaces or next hops based on source, destination, application, or service.
Device-ID Integration: PBF supports source IP, zones, users, and applications but does not include device objects as a match criterion in PAN-OS documentation up to version 10.2. Device-ID is not listed as a supported attribute for PBF rules.
Limitations: PBF focuses on routing, not device-specific enforcement.
Fit: Not supported.
Reference: PAN-OS PBF Configuration (docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/policy- based-forwarding).
D). SD-WAN
Description: SD-WAN policies (Policies > SD-WAN) optimize WAN traffic across multiple links, using application and performance metrics (requires SD-WAN subscription).
Device-ID Integration: SD-WAN policies focus on link selection and application performance, not device attributes. Device-ID is not a match criterion in SD-WAN rules per PAN-OS 10.2 documentation.
Limitations: SD-WAN leverages App-ID and path quality, not device classification.
Fit: Not supported.
Reference: PAN-OS SD-WAN Policies (docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/sd-wan).
E). Quality of Service (QoS)
Description: QoS policies (Policies > QoS) prioritize, limit, or guarantee bandwidth for traffic based on source, destination, application, or user.
Device-ID Integration: QoS policies support device objects as match criteria, allowing bandwidth control based on device type (e.g., prioritize "VoIP Phones" over "Smart TVs").
Example: Limiting bandwidth for IoT devices to prevent network congestion.
Fit: Supported and aligns with Device-ID's purpose.
Reference: PAN-OS QoS with Device-ID (docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/quality-of- service/configure-qos-policy#device-id).
Step 4: Select the Three Policies
Based on PAN-OS capabilities:
Security (A): Device-ID enhances security rules with device-based enforcement.
Decryption (B): Device-ID allows selective decryption based on device classification.
Quality of Service (E): Device-ID enables device-specific bandwidth management.
Why not C or D?
PBF (C): Lacks Device-ID support, focusing on routing rather than device attributes.
SD-WAN (D): Prioritizes link performance over device classification.
Step 5: Verification with Palo Alto Documentation
Security: Explicitly supports Device-ID (PAN-OS Policy Docs).
Decryption: Confirmed in PAN-OS 10.0+ (Decryption Docs).
QoS: Device-ID integration documented (QoS Docs).
PBF and SD-WAN: No mention of Device-ID in policy match criteria (PBF and SD-WAN Docs).
Thus, the verified answers are A, B, E.

NEW QUESTION # 42
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 - The default setting must be changed from no limit to 120 minutes.
- B. No - The PAN-OS XML API does not support keys.
- C. No - The API keys can be made, but there is no method to deactivate them based on time.

- D. Yes - This is the default setting for API keys.

Answer: A

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 theWeb InterfaceorCLIon the firewall.
* Navigate toDevice > 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 # 43
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. SaaS Security
- C. Enterprise DLP
- D. Advanced WildFire
- E. Advanced URL Filtering

Answer: A,D,E

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 # 44
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. Management Data Plane Separation
- B. Parallel Processing
- C. Advanced Routing Engine
- D. Single Pass Architecture

Answer: B,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 # 45
......

We are confident about our Palo Alto Networks PSE-Strata-Pro-24 braindumps tested by our certified experts who have great reputation in IT certification. These PSE-Strata-Pro-24 exam pdf offers you a chance to get high passing score in formal test and help you closer to your success. Valid PSE-Strata-Pro-24 Test Questions can be access and instantly downloaded after purchased and there are free PSE-Strata-Pro-24 pdf demo for you to check.

PSE-Strata-Pro-24 Exam Success: https://www.braindumpspass.com/Palo-Alto-Networks/PSE-Strata-Pro-24-practice-exam-dumps.html

- Best PSE-Strata-Pro-24 Practice □ PSE-Strata-Pro-24 Guaranteed Questions Answers □ Trustworthy PSE-Strata-Pro-24 Pdf □ Immediately open ➤ www.examcollectionpass.com □ and search for ▹ PSE-Strata-Pro-24 ◃ to obtain a free download □PSE-Strata-Pro-24 Dump
- PSE-Strata-Pro-24 Testdump □ Trustworthy PSE-Strata-Pro-24 Pdf □ PSE-Strata-Pro-24 Real Dumps □ Simply search for （ PSE-Strata-Pro-24 ） for free download on 【 www.pdfvce.com 】 □PSE-Strata-Pro-24 Latest Learning Materials
- 2026 100% Free PSE-Strata-Pro-24 –Efficient 100% Free Valid Exam Fee | Palo Alto Networks Systems Engineer Professional - Hardware Firewall Exam Success □ Search for ➡ PSE-Strata-Pro-24 □□□ and download it for free immediately on □ www.exam4labs.com □ □PSE-Strata-Pro-24 Exam Guide
- Top PSE-Strata-Pro-24 Valid Exam Fee – The Newest Exam Success Providers for Palo Alto Networks PSE-Strata-Pro-

24 □ Go to website 「 www.pdfvce.com 」 open and search for □ PSE-Strata-Pro-24 □ to download for free □ □Reliable PSE-Strata-Pro-24 Braindumps Ppt

- PSE-Strata-Pro-24 Dump □ PSE-Strata-Pro-24 Exam Certification □ Trustworthy PSE-Strata-Pro-24 Pdf □ Download （ PSE-Strata-Pro-24 ） for free by simply entering 「 www.troytecdumps.com 」 website □Best PSE-Strata-Pro-24 Practice
- Free PDF Quiz Palo Alto Networks - PSE-Strata-Pro-24 - Palo Alto Networks Systems Engineer Professional - Hardware Firewall Newest Valid Exam Fee □ Go to website ⇛ www.pdfvce.com ⇚ open and search for ➡ PSE-Strata-Pro-24 □□□ to download for free □PSE-Strata-Pro-24 Real Dumps
- Reliable PSE-Strata-Pro-24 Dumps Free □ Reliable PSE-Strata-Pro-24 Exam Syllabus □ PSE-Strata-Pro-24 Test Free ⊙ Download □ PSE-Strata-Pro-24 □ for free by simply searching on □ www.troytecdumps.com □ □PSE-Strata-Pro-24 Testdump
- Top PSE-Strata-Pro-24 Valid Exam Fee – The Newest Exam Success Providers for Palo Alto Networks PSE-Strata-Pro-24 ▤ Search for □ PSE-Strata-Pro-24 □ and download it for free on 「 www.pdfvce.com 」 website □Reliable PSE-Strata-Pro-24 Dumps Free
- 2026 100% Free PSE-Strata-Pro-24 –Reliable 100% Free Valid Exam Fee | Palo Alto Networks Systems Engineer Professional - Hardware Firewall Exam Success □ 【 www.prepawaypdf.com 】 is best website to obtain ➻ PSE-Strata-Pro-24 □ for free download ↔Best PSE-Strata-Pro-24 Practice
- Use Palo Alto Networks PSE-Strata-Pro-24 Dumps to Have Great Outcomes In Palo Alto Networks Exam □ Enter ✔ www.pdfvce.com □✔□ and search for 【 PSE-Strata-Pro-24 】 to download for free □PSE-Strata-Pro-24 Exam Tutorial
- Free PDF Quiz Palo Alto Networks - PSE-Strata-Pro-24 - Palo Alto Networks Systems Engineer Professional - Hardware Firewall Newest Valid Exam Fee □ Simply search for □ PSE-Strata-Pro-24 □ for free download on ▸ www.prepawaypdf.com ◂ □PSE-Strata-Pro-24 Examcollection Questions Answers
- myportal.utt.edu.tt, bbs.t-firefly.com, knowyourmeme.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, bbs.t-firefly.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, Disposable vapes

DOWNLOAD the newest BraindumpsPass PSE-Strata-Pro-24 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1fR-mYswQacRGOLDsk4LaXnOr2Z4XsqHt