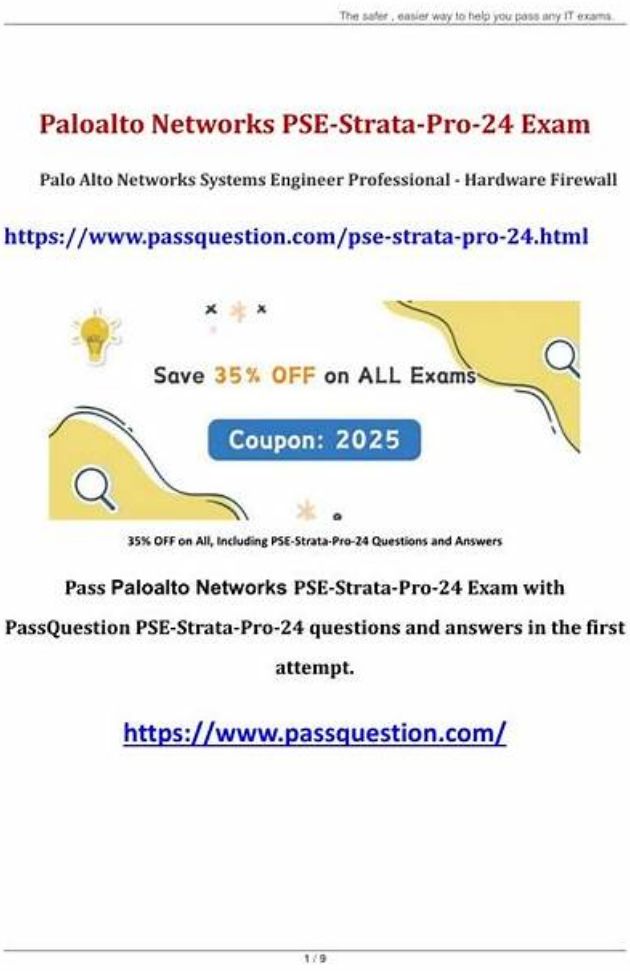
Palo Alto Networks PSE-Strata-Pro-24 Exam Actual Questions - Latest PSE-Strata-Pro-24 Test Online



BONUS!!! Download part of BraindumpStudy PSE-Strata-Pro-24 dumps for free: https://drive.google.com/open?id=1TJwnPc1JqtCvxBHZWmdi985b80mvRAAb

As we know, if you can obtain the job qualification PSE-Strata-Pro-24 certificate, which shows you have acquired many skills. In this way, your value is greatly increased in your company. Then sooner or later you will be promoted by your boss. Our PSE-Strata-Pro-24 Preparation exam really suits you best for your requirement. We have been considered to be the best friend for helping numerous of our customers successfully get their according PSE-Strata-Pro-24 certification.

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	• 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 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	• 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.

Varieties of Palo Alto Networks PSE-Strata-Pro-24 Exam Practice Test Questions

Do you upset about the difficulty of Palo Alto Networks practice questions? Do you disappointed at losing exam after long-time preparation? We can help you from these troubles with our Latest PSE-Strata-Pro-24 Learning Materials and test answers. You will find valid PSE-Strata-Pro-24 real questions and detailed explanations in BraindumpStudy, which ensure you clear exam easily.

Palo Alto Networks Systems Engineer Professional - Hardware Firewall Sample Questions (Q14-Q19):

NEW QUESTION # 14
Which three use cases are specific to Policy Optimizer? (Choose three.)

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

Answer: B,D,E

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.
Reference: PAN-OS Administrator's Guide (11.1) - Policy Optimizer Overview

"Policy Optimizer simplifies the transition to application-based policies, optimizes existing rules, and provides visibility into application usage." Step 2: Evaluating the Use Cases Option A: Discovering applications on the network and transitions to application-based policy over time Analysis: Policy Optimizer's New App Viewer feature discovers applications by analyzing traffic logs (e.
g., Monitor > Logs > Traffic) against rules allowing "any" application or port-based rules. It lists applications seen on the network, enabling administrators to gradually replace broad rules with specific App-IDs over time.
How It Works:
Identify a rule (e.g., "allow TCP/443").
New App Viewer shows apps like "web-browsing" or "salesforce" hitting that rule.
Replace "any" with specific App-IDs, refining the policy incrementally.
Why Specific: This discovery and transition process is a core Policy Optimizer function, unique to its workflow.
Conclusion: Correct use case.
Reference: PAN-OS Administrator's Guide (11.1) - New App Viewer
"Use New App Viewer to discover applications and transition to App-ID-based policies." Option B: Converting broad rules based on application filters into narrow rules based on application groups Analysis: Application filters (e.g., "web-based") are dynamic categories in PAN-OS, while application groups are static lists of specific App-IDs (e.g., "web-browsing, ssl"). Policy Optimizer doesn't convert filters to groups-it focuses on replacing "any" or port-based rules with specific App-IDs or groups, not refining filters. This task is more manual or aligns with general policy management, not a Policy Optimizer-specific feature.
Conclusion: Not a specific use case.
Reference: PAN-OS Administrator's Guide (11.1) - Application Filters vs. Groups
"Policy Optimizer targets port-to-App-ID transitions, not filter-to-group conversions." Option C: Enabling migration from port-based rules to application-based rules Analysis: A flagship use case for Policy Optimizer is migrating legacy port-based rules (e.g., "allow TCP
/80") to App-ID-based rules (e.g., "allow web-browsing"). The Port-Based Rule Usage tab identifies rules using ports, tracks associated traffic, and suggests App-IDs based on logs.
How It Works:
View port-based rules in Policies > Policy Optimizer > Port Based Rules.
Analyze traffic to see apps (e.g., "http-video" on TCP/80).
Convert the rule to use App-IDs, enhancing security and visibility.
Why Specific: This migration is a hallmark of Policy Optimizer, addressing legacy firewall designs.
Conclusion: Correct use case.
Reference: PAN-OS Administrator's Guide (11.1) - Migrate Port-Based to App-ID-Based Rules
"Policy Optimizer facilitates migration from port-based to application-based security policies." Option D: Discovering 5-tuple attributes that can be simplified to 4-tuple attributes Analysis: A 5-tuple (source IP, destination IP, source port, destination port, protocol) defines a flow, while a 4-tuple omits one element (e.g., source port). Policy Optimizer doesn't focus on tuple simplification-it analyzes applications and rule usage, not low-level flow attributes. Tuple management is more relevant to NAT or QoS, not Policy Optimizer.
Conclusion: Not a specific use case.
Reference: PAN-OS Administrator's Guide (11.1) - Traffic Logs
"Policy Optimizer works at the application layer, not tuple simplification." Option E: Automating the tagging of rules based on historical log data Analysis: Policy Optimizer's Rule Usage feature tracks rule hits and unused rules over time (e.g., 30 days), allowing automated tagging (e.g., "unused" or "high-traffic") based on historical logs. This helps prioritize rule optimization or cleanup.
How It Works:
Enable Rule Usage tracking (Policies > Policy Optimizer > Rule Usage).
Logs populate hit counts and last-used timestamps.
Auto-tag rules (e.g., "No Hits in 90 Days") for review.
Why Specific: Automated tagging based on log history is a unique Policy Optimizer capability for rule management.
Conclusion: Correct use case.
Reference: PAN-OS Administrator's Guide (11.1) - Rule Usage
"Automate rule tagging based on historical usage to optimize policies." Step 3: Why A, C, and E Are Correct A: Discovers applications and supports a phased transition to App-ID policies, a proactive optimization step.
C: Directly migrates port-based rules to App-ID-based rules, addressing legacy configurations.
E: Automates rule tagging using log data, streamlining policy maintenance.These align with Policy Optimizer's purpose of enhancing visibility, security, and efficiency on Strata NGFWs.
Step 4: Exclusion Rationale
B: Filter-to-group conversion isn't a Policy Optimizer feature-it's a manual policy design choice.
D: Tuple simplification isn't within Policy Optimizer's scope, which focuses on applications, not flow attributes.

NEW QUESTION # 15
In which two locations can a Best Practice Assessment (BPA) report be generated for review by a customer?

(Choose two.)

- A. Strata Cloud Manager (SCM)
- B. Customer Support Portal
- C. PANW Partner Portal
- D. AIOps

Answer: A,D

Explanation:
Step 1: Understand the Best Practice Assessment (BPA)
* Purpose: The BPA assesses NGFW (e.g., PA-Series) and Panorama configurations against best practices, including Center for Internet Security (CIS) Critical Security Controls, to enhance security and feature adoption.
* Process: Requires a Tech Support File (TSF) upload or telemetry data from onboarded devices to generate the report.
* Evolution: Historically available via the Customer Support Portal, the BPA has transitioned to newer platforms like AIOps and Strata Cloud Manager.
"BPA measures security posture against best practices" (paloaltonetworks.com, Best Practice Assessment Overview).
Step 2: Evaluate Each Option
Option A: PANW Partner Portal
Description: The Palo Alto Networks Partner Portal is a platform for partners (e.g., resellers, distributors) to access tools, resources, and customer-related services.
BPA Capability:
Historically, partners could generate BPAs on behalf of customers via the Customer Success Portal (accessible through Partner Portal integration), but this was not a direct customer-facing feature.
As of July 17, 2023, the BPA generation capability in the Customer Support Portal and related partner tools was disabled, shifting focus to AIOps and Strata Cloud Manager.
Partners can assist customers with BPA generation but cannot directly generate reports for customer review in the Partner Portal itself; customers must access reports via their own interfaces (e.g., AIOps).
Verification:
"BPA transitioned to AIOps; Customer Support Portal access disabled after July 17, 2023" (live.paloaltonetworks.com, BPA Transition Announcement, 07-10-2023).
No current documentation supports direct BPA generation in the Partner Portal for customer review.
Conclusion: Not a customer-accessible location for generating BPAs. Not Applicable.
Option B: Customer Support Portal
Description: The Customer Support Portal (support.paloaltonetworks.com) provides customers with tools, case management, and historically, BPA generation.
BPA Capability:
Prior to July 17, 2023, customers could upload a TSF under "Tools > Best Practice Assessment" to generate a BPA report (HTML, XLSX, PDF formats).
Post-July 17, 2023, this functionality was deprecated in favor of AIOps and Strata Cloud Manager. Historical BPA data was maintained until December 31, 2023, but new report generation ceased.
As of March 08, 2025, the Customer Support Portal no longer supports BPA generation, though it remains a support hub.
Verification:
"TSF uploads for BPA in Customer Support Portal disabled after July 17, 2023" (docs.paloaltonetworks.com/panorama/10-2/panorama-admin/panorama-best-practices).
"Transition to AIOps for BPA generation" (live.paloaltonetworks.com, BPA Transition to AIOps, 07-10-2023).
Conclusion: No longer a valid location for BPA generation as of the current date. Not Applicable.
Option C: AIOps
Description: AIOps for NGFW is an AI-powered operations platform for managing Strata NGFWs and Panorama, offering real-time insights, telemetry-based monitoring, and BPA generation.
BPA Capability:
Supports two BPA generation methods:
On-Demand BPA: Customers upload a TSF (PAN-OS 9.1 or higher) via "Dashboards > On Demand BPA" to generate a report, even without telemetry or onboarding.
Continuous BPA: For onboarded devices with telemetry enabled (PAN-OS 10.0+), AIOps provides ongoing best practice assessments via the Best Practices dashboard.
Available in free and premium tiers; the free tier includes BPA generation.
Reports include detailed findings, remediation steps, and adoption summaries.
Use Case: Ideal for customers managing firewalls with or without full AIOps integration.
Verification:

"Generate on-demand BPA reports by uploading TSFs in AIOps" (docs.paloaltonetworks.com/aiops/aiops-for-ngfw/dashboards/on-demand-bpa).
"AIOps Best Practices dashboard assesses configurations continuously" (live.paloaltonetworks.com, AIOps On-Demand BPA, 10-25-2022).
Conclusion: A current, customer-accessible location for BPA generation. Applicable.
Option D: Strata Cloud Manager (SCM)
Description: Strata Cloud Manager is a unified, AI-powered management interface for NGFWs and SASE, integrating AIOps, digital experience management, and configuration tools.
BPA Capability:
Supports on-demand BPA generation by uploading a TSF under "Dashboards > On Demand BPA," similar to AIOps, for devices not sending telemetry or not fully onboarded.
For onboarded devices, provides real-time best practice checks via the "Best Practices" dashboard, analyzing policies against Palo Alto Networks and CIS standards.
Available in Essentials (free) and Pro (paid) tiers; BPA generation is included in both.
Use Case: Offers a modern, centralized platform for customers to manage and assess security posture.
Verification:
"Run BPA directly from Strata Cloud Manager with TSF upload" (docs.paloaltonetworks.com/strata-cloud-manager/dashboards/on-demand-bpa, 07-24-2024).
"Best Practices dashboard measures posture against guidance" (paloaltonetworks.com, Strata Cloud Manager Overview).
Conclusion: A current, customer-accessible location for BPA generation. Applicable.
Step 3: Select the Two Valid Locations
C (AIOps): Supports both on-demand (TSF upload) and continuous BPA generation, accessible to customers via the Palo Alto Networks hub.
D (Strata Cloud Manager): Provides identical on-demand BPA capabilities and real-time assessments, designed as a unified management interface.
Why Not A or B?
A (PANW Partner Portal): Partner-focused, not a direct customer tool for BPA generation.
B (Customer Support Portal): Deprecated for BPA generation post-July 17, 2023; no longer valid as of March 08, 2025.
Step 4: Verified References
AIOps BPA: "On-demand BPA in AIOps via TSF upload" (docs.paloaltonetworks.com/aiops/aiops-for-ngfw /dashboards/on-demand-bpa).
Strata Cloud Manager BPA: "Generate BPA reports in SCM" (docs.paloaltonetworks.com/strata-cloud- manager/dashboards/on-demand-bpa).
Customer Support Portal Transition: "BPA moved to AIOps/SCM; CSP access ended July 17, 2023" (live. paloaltonetworks.com, BPA Transition, 07-10-2023).

NEW QUESTION # 16
An existing customer wants to expand their online business into physical stores for the first time. The customer requires NGFWs at the physical store to handle SD-WAN, security, and data protection needs, while also mandating a vendor-validated deployment method. Which two steps are valid actions for a systems engineer to take? (Choose two.)

- A. Use Golden Images and Day 1 configuration to create a consistent baseline from which the customer can efficiently work.
- B. Recommend the customer purchase Palo Alto Networks or partner-provided professional services to meet the stated requirements.
- C. Use the reference architecture "On-Premises Network Security for the Branch Deployment Guide" to achieve a desired architecture.
- D. Create a bespoke deployment plan with the customer that reviews their cloud architecture, store footprint, and security requirements.

Answer: B,C

Explanation:
When an existing customer expands their online business into physical stores and requires Next-Generation Firewalls (NGFWs) at those locations to handle SD-WAN, security, and data protection-while mandating a vendor-validated deployment method-a systems engineer must leverage Palo Alto Networks' Strata Hardware Firewall capabilities and validated deployment strategies. The Strata portfolio, particularly the PA- Series NGFWs, is designed to secure branch offices with integrated SD-WAN and robust security features.
Below is a detailed explanation of why options A and D are the correct actions, grounded in Palo Alto Networks' documentation and practices as of March 08, 2025.
Step 1: Recommend Professional Services (Option A)

The customer's requirement for a "vendor-validated deployment method" implies a need for expertise and assurance that the solution meets their specific needs-SD-WAN, security, and data protection-across new physical stores. Palo Alto Networks offers professional services, either directly or through certified partners, to ensure proper deployment of Strata Hardware Firewalls like the PA-400 Series or PA-1400 Series, which are ideal for branch deployments. These services provide end-to-end support, from planning to implementation, aligning with the customer's mandate for a validated approach.
* Professional Services Scope:Palo Alto Networks' professional services include architecture design, deployment, and optimization for NGFWs and SD-WAN. This ensures that the PA-Series firewalls are configured to handle SD-WAN (e.g., dynamic path selection), security (e.g., Threat Prevention with ML-powered inspection), and data protection (e.g., WildFire for malware analysis and Data Loss Prevention integration).
* Vendor Validation:By recommending these services, the engineer ensures a deployment that adheres to Palo Alto Networks' best practices, meeting the customer's requirement for a vendor-validated method. This is particularly critical for a customer new to physical store deployments, as it mitigates risks and accelerates time-to-value.
* Strata Hardware Relevance:The PA-410, for example, is a desktop NGFW designed for small branch offices, offering SD-WAN and Zero Trust security out of the box. Professional services ensure its correct integration into the customer's ecosystem.

NEW QUESTION # 17
Which two statements clarify the functionality and purchase options for Palo Alto Networks AIOps for NGFW? (Choose two.)

- A. It uses telemetry data to forecast, preempt, or identify issues, and it uses machine learning (ML) to adjust and enhance the process.
- B. It is offered in two license tiers: a free version and a premium version.
- C. It is offered in two license tiers: a commercial edition and an enterprise edition.
- D. It forwards log data to Advanced WildFire to anticipate, prevent, or identify issues, and it uses machine learning (ML) to refine and adapt to the process.

Answer: A,B

Explanation:
Palo Alto Networks AIOps for NGFW is a cloud-delivered service that leverages telemetry data and machine learning (ML) to provide proactive operational insights, best practice recommendations, and issue prevention.
* Why "It is offered in two license tiers: a free version and a premium version" (Correct Answer B)?AIOps for NGFW is available in two tiers:
* Free Tier: Provides basic operational insights and best practices at no additional cost.
* Premium Tier: Offers advanced capabilities, such as AI-driven forecasts, proactive issue prevention, and enhanced ML-based recommendations.
* Why "It uses telemetry data to forecast, preempt, or identify issues, and it uses machine learning (ML) to adjust and enhance the process" (Correct Answer C)?AIOps uses telemetry data from NGFWs to analyze operational trends, forecast potential problems, and recommend solutions before issues arise. ML continuously refines these insights by learning from real-world data, enhancing accuracy and effectiveness over time.
* Why not "It is offered in two license tiers: a commercial edition and an enterprise edition" (Option A)?This is incorrect because the licensing model for AIOps is based on "free" and "premium" tiers, not "commercial" and "enterprise" editions.
* Why not "It forwards log data to Advanced WildFire to anticipate, prevent, or identify issues, and it uses machine learning (ML) to refine and adapt to the process" (Option D)?AIOps does not rely on Advanced WildFire for its operation. Instead, it uses telemetry data directly from the NGFWs to perform operational and security analysis.
Reference: Palo Alto Networks documentation for AIOps for NGFW confirms its functionality and licensing structure.

NEW QUESTION # 18
What are three valid Panorama deployment options? (Choose three.)

- A. As a virtual machine (ESXi, Hyper-V, KVM)
- B. With a cloud service provider (AWS, Azure, GCP)
- C. As a dedicated hardware appliance (M-100, M-200, M-500, M-600)
- D. On a Raspberry Pi (Model 4, Model 400, Model 5)
- E. As a container (Docker, Kubernetes, OpenShift)

Answer: A,B,C

Explanation:
Panorama is Palo Alto Networks' centralized management solution for managing multiple firewalls. It supports multiple deployment

options to suit different infrastructure needs. The valid deployment options are as follows:
* Why "As a virtual machine (ESXi, Hyper-V, KVM)" (Correct Answer A)?Panorama can be deployed as a virtual machine on hypervisors like VMware ESXi, Microsoft Hyper-V, and KVM. This is a common option for organizations that already utilize virtualized infrastructure.
* Why "With a cloud service provider (AWS, Azure, GCP)" (Correct Answer B)?Panorama is available for deployment in the public cloud on platforms like AWS, Microsoft Azure, and Google Cloud Platform. This allows organizations to centrally manage firewalls deployed in cloud environments.
* Why "As a dedicated hardware appliance (M-100, M-200, M-500, M-600)" (Correct Answer E)?
Panorama is available as a dedicated hardware appliance with different models (M-100, M-200, M-500, M-600) to cater to various performance and scalability requirements. This is ideal for organizations that prefer physical appliances.
* Why not "As a container (Docker, Kubernetes, OpenShift)" (Option C)?Panorama is not currently supported as a containerized deployment. Containers are more commonly used for lightweight and ephemeral services, whereas Panorama requires a robust and persistent deployment model.
* Why not "On a Raspberry Pi (Model 4, Model 400, Model 5)" (Option D)?Panorama cannot be deployed on low-powered hardware like Raspberry Pi. The system requirements for Panorama far exceed the capabilities of Raspberry Pi hardware.
Reference: Palo Alto Networks Panorama Admin Guide outlines the supported deployment options, which include virtual machines, cloud platforms, and hardware appliances.

NEW QUESTION # 19
.....

Strata-Pro-24 Format

- learn.eggdemy.com, www.stes.tyc.edu.tw, learn.designoriel.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, tadika.israk.my, adamree449.blogdeazar.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, shortcourses.russellcollege.edu.au, worksmarter.com.au, ascentleadershipinstitute.org, Disposable vapes

What's more, part of that BraindumpStudy PSE-Strata-Pro-24 dumps now are free: https://drive.google.com/open?id=1TJwnPc1JqtCvxBHZWmdi985b80mvRAAb