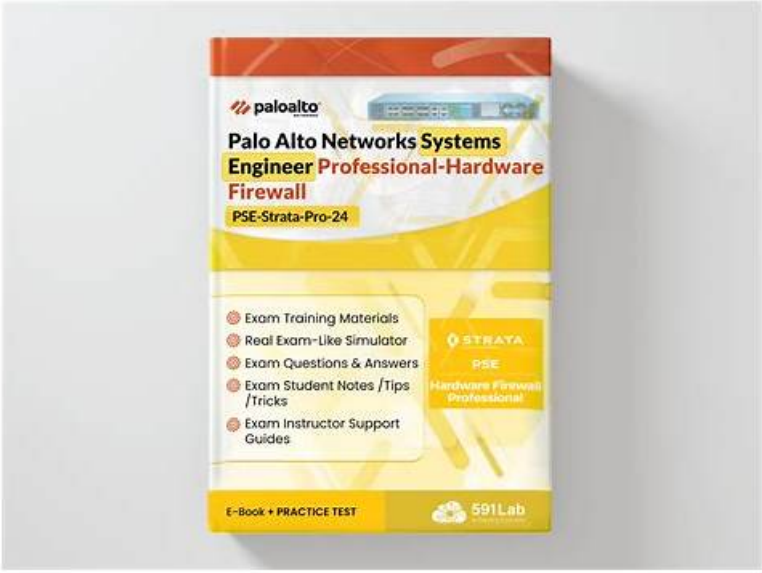
PSE-Strata-Pro-24試験の準備方法｜ユニークなPSE-Strata-Pro-24技術問題試験｜認定するPalo Alto Networks Systems Engineer Professional - Hardware Firewall試験問題解説集



P.S.GoShikenがGoogle Driveで共有している無料の2026 Palo Alto Networks PSE-Strata-Pro-24ダンプ：https://drive.google.com/open?id=1p4ucCVQMDvoNFmdv9tTfV2guYtu9wCDQ

GoShikenを選択したら100%PSE-Strata-Pro-24試験に合格することができます。試験科目の変化によって、最新のPSE-Strata-Pro-24試験の内容も更新いたします。GoShikenのインターネットであなたに年24時間のオンライン顧客サービスを無料で提供して、もしあなたはGoShikenに失敗したら、弊社が全額で返金いたします。

PSE-Strata-Pro-24試験の質問は、当社の製品を使用して試験を準備し、夢の証明書を取得できると信じています。より良い求人を希望する場合は、適切なプロ品質を備えなければならないことを私たちは皆知っています。私たちのPSE-Strata-Pro-24学習教材はあなたのそばにいて気配りのあるサービスを提供する用意があります、そして私たちのPSE-Strata-Pro-24学習教材はすべてのお客様に心からお勧めします。想像できる。 PSE-Strata-Pro-24トレーニングガイドには多くの利点があります。

>> PSE-Strata-Pro-24技術問題 <<

理解安いPSE-Strata-Pro-24技術問題: Palo Alto Networks Systems Engineer Professional - Hardware Firewall心配する必要はありません

GoShiken提供した商品の品質はとても良くて、しかも更新のスピードももっともはやくて、もし君はPalo Alto NetworksのPSE-Strata-Pro-24の認証試験に関する学習資料をしっかり勉強して、成功することも簡単になります。

Palo Alto Networks PSE-Strata-Pro-24 認定試験の出題範囲:

トピック	出題範囲
トピック 1	• 導入と評価: この試験セクションでは、導入エンジニアのスキルを測定し、Palo Alto Networks NGFW の機能の特定に重点が置かれます。受験者は、既知と未知の両方の脅威から保護する機能を評価します。また、導入の観点から ID 管理を説明し、NGFW ソリューションの有効性の評価を含む価値証明 (PoV) プロセスについても説明します。

トピック 2	• アーキテクチャと計画: この試験セクションでは、ネットワーク アーキテクトのスキルを測定し、顧客の要件を理解し、適切な導入アーキテクチャを設計することに重点が置かれます。受験者は、Palo Alto Networks のプラットフォーム ネットワーキング機能を詳細に説明し、さまざまな環境への適合性を評価する必要があります。システムのサイズ設定や微調整などの側面の処理も、この分野で評価される重要なスキルです。
トピック 3	• ビジネス価値と競争上の差別化要因: この試験セクションでは、テクニカル ビジネス価値アナリストのスキルを測定し、Palo Alto Networks 次世代ファイアウォール (NGFW) の価値提案の特定に重点を置きます。受験者は、Panorama や SCM などのツールの技術的なビジネス上の利点を評価します。また、顧客に関連するトピックを認識し、それを Palo Alto Networks の最適なソリューションに合わせます。さらに、Strata 独自の差別化要因を理解することは、このドメインの重要な要素です。
トピック 4	• ネットワーク セキュリティ戦略とベスト プラクティス: この試験セクションでは、セキュリティ戦略スペシャリストのスキルを測定し、Palo Alto Networks の 5 段階のゼロ トラスト手法の重要性を強調します。受験者は、堅牢なネットワーク セキュリティを確保するためのベスト プラクティスを重視しながら、ゼロ トラスト モデルに効果的にアプローチして適用する方法を理解する必要があります。

Palo Alto Networks Systems Engineer Professional - Hardware Firewall 認定 PSE-Strata-Pro-24 試験問題 (Q59-Q64):

質問 # 59
Which three use cases are specific to Policy Optimizer? (Choose three.)

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

正解：A、C、D

解説：
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.

質問 # 60
A prospective customer is interested in Palo Alto Networks NGFWs and wants to evaluate the ability to segregate its internal network into unique BGP environments.
Which statement describes the ability of NGFWs to address this need?

- A. It cannot be addressed because PAN-OS does not support it.
- B. It can be addressed by creating multiple eBGP autonomous systems.
- C. It can be addressed with BGP confederations.
- D. It cannot be addressed because BGP must be fully meshed internally to work.

正解：C

解説：

Step 1: Understand the Requirement and Context
* Customer Need: Segregate the internal network into unique BGP environments, suggesting multiple isolated or semi-isolated routing domains within a single organization.
* BGP Basics:
* BGP is a routing protocol used to exchange routing information between autonomous systems (ASes).
* eBGP: External BGP, used between different ASes.
* iBGP: Internal BGP, used within a single AS, typically requiring a full mesh of peers unless mitigated by techniques like confederations or route reflectors.
* Palo Alto NGFW: Supports BGP on virtual routers (VRs) within PAN-OS, enabling advanced routing capabilities for Strata hardware firewalls (e.g., PA-Series).
* "PAN-OS supports BGP for dynamic routing and network segmentation" (docs.paloaltonetworks.com/pan-os /10-2/pan-os-networking-admin/bgp).
Step 2: Evaluate Each Option
Option A: It cannot be addressed because PAN-OS does not support it
Analysis:
PAN-OS fully supports BGP, including eBGP, iBGP, confederations, and route reflectors, configurable under "Network > Virtual Routers > BGP."
Features like multiple virtual routers and BGP allow network segregation and routing policy control.
This statement contradicts documented capabilities.
Verification:
"Configure BGP on a virtual router for dynamic routing" (docs.paloaltonetworks.com/pan-os/10-2/pan-os- networking-admin/bgp/configure-bgp).
Conclusion: Incorrect-PAN-OS supports BGP and segregation techniques. Not Applicable.
Option B: It can be addressed by creating multiple eBGP autonomous systems Analysis:
eBGP: Used between distinct ASes, each with a unique AS number (e.g., AS 65001, AS 65002).
Within a single organization, creating multiple eBGP ASes would require:
Assigning unique AS numbers (public or private) to each internal segment.
Treating each segment as a separate AS, peering externally with other segments via eBGP.
Challenges:
Internally, this isn't practical for a single network-it's more suited to external peering (e.g., with ISPs).
Requires complex management and public/private AS number allocation, not ideal for internal segregation.
Doesn't leverage iBGP or confederations, which are designed for internal AS management.
PAN-OS supports eBGP, but this approach misaligns with the intent of internal network segregation.
Verification:
"eBGP peers connect different ASes" (docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/bgp /bgp-concepts).
Conclusion: Possible but impractical and not the intended BGP solution for internal segregation. Not Optimal

質問 # 61
Which three descriptions apply to a perimeter firewall? (Choose three.)

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

正解：A、B、E

解説：
A perimeter firewall is 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 provide network layer protection by 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 with data center firewalls, which monitor 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 secures north-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 in guarding 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.

質問 # 62
A company with a large Active Directory (AD) of over 20,000 groups has user roles based on group membership in the directory. Up to 1,000 groups may be used in Security policies. The company has limited operations personnel and wants to reduce the administrative overhead of managing the synchronization of the groups with their firewalls.
What is the recommended architecture to synchronize the company's AD with Palo Alto Networks firewalls?

- A. Configure a group mapping profile with custom filters for LDAP attributes that are mapped to the user roles.
- B. Configure NGFWs to synchronize with the AD after deploying the Cloud Identity Engine (CIE) and agents.
- C. Configure a group mapping profile with an include group list.
- D. Configure a group mapping profile, without a filter, to synchronize all groups.

正解：C

解説：
Synchronizing a large Active Directory (AD) with over 20,000 groups can introduce significant overhead if all groups are synchronized, especially when only a subset of groups (e.g., 1,000 groups) are required for Security policies. The most efficient approach is to configure agroupmapping profile with an include group listto minimize unnecessary synchronization and reduce administrative overhead.
* Why "Configure a group mapping profile with an include group list" (Correct Answer C)?Using a group mapping profile with aninclude group listensures that only the required 1,000 groups are synchronized with the firewall. This approach:
* Reduces the load on the firewall's User-ID process by limiting the number of synchronized groups.
* Simplifies management by focusing on the specific groups relevant to Security policies.
* Avoids synchronizing the entire directory (20,000 groups), which would be inefficient and resource-intensive.
* Why not "Configure a group mapping profile, without a filter, to synchronize all groups" (Option B)?Synchronizing all 20,000 groups would unnecessarily increase administrative and resource overhead. This approach contradicts the requirement to reduce administrative burden.
* Why not "Configure a group mapping profile with custom filters for LDAP attributes that are mapped to the user roles" (Option A)?While filtering LDAP attributes can be useful, this approach is more complex to implement and manage compared to an include group list. It does not directly address the problem of limiting synchronization to a specific subset of groups.
* Why not "Configure NGFWs to synchronize with the AD after deploying the Cloud Identity Engine (CIE) and agents" (Option D)? While the Cloud Identity Engine (CIE) is a modern solution for user and group mapping, it is unnecessary in this scenario. A traditional group mapping profile with an include list is sufficient and simpler to implement. CIE is typically used for complex hybrid or cloud environments.

質問 # 63
Which two tools should a systems engineer use to showcase the benefit of an evaluation that a customer has just concluded?

- A. Best Practice Assessment (BPA)
- B. Golden Images
- C. Security Lifecycle Review (SLR)
- D. Firewall Sizing Guide

正解：A、C

解説：
After a customer has concluded an evaluation of Palo Alto Networks solutions, it is critical to provide a detailed analysis of the results and benefits gained during the evaluation. The following two tools are most appropriate:
* Why "Best Practice Assessment (BPA)" (Correct Answer A)?The BPA evaluates the customer's firewall configuration against Palo Alto Networks' recommended best practices. It highlights areas where the configuration could be improved to strengthen security posture. This is an excellent tool to showcase how adopting Palo Alto Networks' best practices aligns with industry standards and improves security performance.
* Why "Security Lifecycle Review (SLR)" (Correct Answer B)?The SLR provides insights into the customer's security environment

based on data collected during the evaluation. It identifies vulnerabilities, risks, and malicious activities observed in the network and demonstrates how Palo Alto Networks' solutions can address these issues. SLR reports use clear visuals and metrics, making it easier to showcase the benefits of the evaluation.
* Why not "Firewall Sizing Guide" (Option C)?The Firewall Sizing Guide is a pre-sales tool used to recommend the appropriate firewall model based on the customer's network size, performance requirements, and other criteria. It is not relevant for showcasing the benefits of an evaluation.
* Why not "Golden Images" (Option D)?Golden Images refer to pre-configured templates for deploying firewalls in specific use cases. While useful for operational efficiency, they are not tools for demonstrating the outcomes or benefits of a customer evaluation.
Reference: Palo Alto Networks documentation for Best Practice Assessment (BPA) and Security Lifecycle Review (SLR) confirms their role in showcasing evaluation benefits.

質問 # 64
.....

我々の提供する資料は高質量で的中率も高いです。このPSE-Strata-Pro-24模擬問題集を利用して、試験に参加するあなたはPSE-Strata-Pro-24試験に合格できると信じています。ご安心に我々の問題集を利用してください。我々はあなたに最大の利便性をもたらすために、一番いいPSE-Strata-Pro-24問題集を提供して、あなたが合格できるのを確保します。

る：https://drive.google.com/open?id=1p4ucCVQMDvoNFmdv9tTfV2guYtu9wCDQ