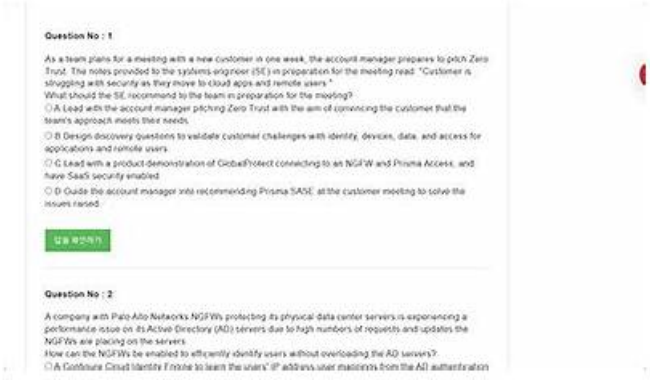
시험준비에가장좋은PSE-Strata-Pro-24높은통과율덤프샘플문제덤프공부자료


Question No : 1

As a team plans for a meeting with a new customer in one week, the account manager prepares to pitch Zero Trust. The notes provided to the systems engineer (SE) in preparation for the meeting read: "Customer is struggling with security as they move to cloud apps and remote users."
What should the SE recommend to the team in preparation for the meeting?
○ A. Lead with the account manager pitching Zero Trust with the aim of convincing the customer that the team's approach meets their needs.
○ B. Design discovery questions to validate customer challenges with identity, devices, data, and access for applications and remote users.
○ C. Lead with a product demonstration of GlobalProtect connecting to an NGFW and Prisma Access, and have SaaS security enabled.
○ D. Guide the account manager into recommending Prisma SASE at the customer meeting to solve the issues raised.

Question No : 2

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

참고: KoreaDumps에서 Google Drive로 공유하는 무료, 최신 PSE-Strata-Pro-24 시험 문제집이 있습니다: https://drive.google.com/open?id=1Lq9nWp22x0y7YyKlA3jMh8b2oIfQDVje

Palo Alto Networks PSE-Strata-Pro-24인증덤프는 최근 출제된 실제시험문제를 바탕으로 만들어진 공부자료입니다. Palo Alto Networks PSE-Strata-Pro-24 시험문제가 변경되면 제일 빠른 시일내에 덤프를 업데이트하여 최신버전 덤프자료를Palo Alto Networks PSE-Strata-Pro-24덤프를 구매한 분들께 보내드립니다. 시험탈락시 덤프비용 전액환불을 약속해드리기에 안심하시고 구매하셔도 됩니다.

Palo Alto Networks PSE-Strata-Pro-24 시험요강:

주제	소개
주제 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.
주제 2	• 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.
주제 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.
주제 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.

>> PSE-Strata-Pro-24높은 통과율 덤프샘플문제 <<

Palo Alto Networks PSE-Strata-Pro-24최고품질 시험대비자료 & PSE-Strata-Pro-24유효한 덤프문제

KoreaDumps는 오래된 IT인증시험덤프를 제공해드리는 전문적인 사이트입니다. KoreaDumps의 Palo Alto Networks 인증 PSE-Strata-Pro-24덤프는 업계에서 널리 알려진 최고품질의Palo Alto Networks인증 PSE-Strata-Pro-24시험대비 자료입니다. Palo Alto Networks인증 PSE-Strata-Pro-24덤프는 최신 시험문제의 시험범위를 커버하고 최신 시험문제 유형을 포함하고 있어 시험패스율이 거의 100%입니다. KoreaDumps의Palo Alto Networks인증 PSE-Strata-Pro-24덤프를 구매하시면 밝은 미래가 보입니다.

최신 PSE-Strata Professional PSE-Strata-Pro-24 무료샘플문제 (Q52-Q57):

질문 # 52
Which statement applies to the default configuration of a Palo Alto Networks NGFW?

- A. The default policy action allows all traffic unless explicitly denied.
- B. The default policy action for intrazone traffic is deny, eliminating implicit trust within a security zone.
- C. Security profiles are applied to all policies by default, eliminating implicit trust of any data traversing the firewall.
- D. The default policy action for interzone traffic is deny, eliminating implicit trust between security zones.

정답：D

설명：
The default configuration of a Palo Alto Networks NGFW includes a set of default security rules that determine how traffic is handled when no explicit rules are defined. Here's the explanation for each option:
* Option A: Security profiles are applied to all policies by default, eliminating implicit trust of any data traversing the firewall
* Security profiles (such as Antivirus, Anti-Spyware, and URL Filtering) are not applied to any policies by default. Administrators must explicitly apply them to security rules.
* This statement is incorrect.
* Option B: The default policy action for intrazone traffic is deny, eliminating implicit trust within a security zone
* By default, traffic within the same zone (intrazone traffic) isallowed. For example, traffic between devices in the "trust" zone is permitted unless explicitly denied by an administrator.
* This statement is incorrect.
* Option C: The default policy action allows all traffic unless explicitly denied
* Palo Alto Networks firewalls do not have an "allow all" default rule. Instead, they include a default "deny all" rule for interzone traffic and an implicit "allow" rule for intrazone traffic.
* This statement is incorrect.
* Option D: The default policy action for interzone traffic is deny, eliminating implicit trust between security zones
* By default, traffic between different zones (interzone traffic) is denied. This aligns with the principle of zero trust, ensuring that no traffic is implicitly allowed between zones.
Administrators must define explicit rules to allow interzone traffic.
* This statement is correct.
References:
* Palo Alto Networks documentation on Security Policy Defaults
* Knowledge Base article on Default Security Rules

질문 # 53
Which two methods are valid ways to populate user-to-IP mappings? (Choose two.)

- A. SCP log ingestion
- B. Captive portal
- C. User-ID
- D. XML API

정답：B,D

설명：
Step 1: Understanding User-to-IP Mappings
User-to-IP mappings are the foundation of User-ID, a core feature of Strata Hardware Firewalls (e.g., PA-400 Series, PA-5400 Series). These mappings link a user's identity (e.g., username) to their device's IP address, enabling policy enforcement based on

user identity rather than just IP. Palo Alto Networks supports multiple methods to populate these mappings, depending on thenetwork environment and authentication mechanisms.
* Purpose:Allows the firewall to apply user-based policies, monitor user activity, and generate user- specific logs.
* Strata Context:On a PA-5445, User-ID integrates with App-ID and security subscriptions to enforce granular access control.

질문 # 54
When a customer needs to understand how Palo Alto Networks NGFWs lower the risk of exploitation by newly announced vulnerabilities known to be actively attacked, which solution and functionality delivers the most value?

- A. Advanced Threat Prevention's command injection and SQL injection functions use inline deep learning against zero-day threats.
- B. Advanced URL Filtering uses machine learning (ML) to learn which malicious URLs are being utilized by the attackers, then block the resulting traffic.
- C. WildFire loads custom OS images to ensure that the sandboxing catches any activity that would affect the customer's environment.
- D. Single Pass Architecture and parallel processing ensure traffic is efficiently scanned against any enabled Cloud-Delivered Security Services (CDSS) subscription.

정답：A

설명:
The most effective way to reduce the risk of exploitation by newly announced vulnerabilities is through Advanced Threat Prevention (ATP). ATP uses inline deep learning to identify and block exploitation attempts, even for zero-day vulnerabilities, in real time.
* Why "Advanced Threat Prevention's command injection and SQL injection functions use inline deep learning against zero-day threats" (Correct Answer B)?Advanced Threat Prevention leverages deep learning models directly in the data path, which allows it to analyze traffic in real time and detect patterns of exploitation, including newly discovered vulnerabilities being actively exploited in the wild.
It specifically targets advanced tactics like:
* Command injection.
* SQL injection.
* Memory-based exploits.
* Protocol evasion techniques.
This functionality lowers the risk of exploitation by actively blocking attack attempts based on their behavior, even when a signature is not yet available. This approach makes ATP the most valuable solution for addressing new and actively exploited vulnerabilities.
* Why not "Advanced URL Filtering uses machine learning (ML) to learn which malicious URLs are being utilized by the attackers, then block the resulting traffic" (Option A)?While Advanced URL Filtering is highly effective at blocking access to malicious websites, it does not provide the inline analysis necessary to prevent direct exploitation of vulnerabilities. Exploitation often happens within the application or protocol layer, which Advanced URL Filtering does not inspect.
* Why not "Single Pass Architecture and parallel processing ensure traffic is efficiently scanned against any enabled Cloud-Delivered Security Services (CDSS) subscription" (Option C)?Single Pass Architecture improves performance by ensuring all enabled services (like Threat Prevention, URL Filtering, etc.) process traffic efficiently. However, it is not a feature that directly addresses vulnerability exploitation or zero-day attack detection.
* Why not "WildFire loads custom OS images to ensure that the sandboxing catches any activity that would affect the customer's environment" (Option D)?WildFire is a sandboxing solution designed to detect malicious files and executables. While it is useful for analyzing malware, it does not provide inline protection against exploitation of newly announced vulnerabilities, especially those targeting network protocols or applications.
Reference: Palo Alto Networks Advanced Threat Prevention specifically highlights its capability to detect and block zero-day exploits, leveraging inline deep learning and machine learning models. This makes it the optimal solution for protecting against new vulnerabilities being actively exploited.

질문 # 55
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. Use Panorama for firewall management and to transfer logs from the 500 firewalls directly to a third- party SIEM for

centralized logging and reporting.
- C. 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.
- D. 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.

정답：D

설명:
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

질문 # 56
Device-ID can be used in which three policies? (Choose three.)

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

정답：B,C,D

설명:
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.

질문 # 57
.....