Download Palo Alto Networks PSE-Strata-Pro-24 Exam Dumps Free

Shared by Melton on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which three use cases are specific to Policy Optimizer? (Select three.)

Options:

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

Answer:

A, B, C

Explanation:

Discovering Applications on the Network (Answer A):

Policy Optimizer analyzes traffic logs to identify applications running on the network that are currently being allowed by port-based or overly permissive policies.

It provides visibility into these applications, enabling administrators to transition to more secure, application-based policies over time.

Converting Broad Rules into Narrow Rules (Answer B):

Policy Optimizer helps refine policies by converting broad application filters (e.g., rules that allow all web applications) into narrower rules based on specific application groups.

This reduces the risk of overly permissive access while maintaining granular control.

Migrating from Port-Based Rules to Application-Based Rules (Answer C):

One of the primary use cases for Policy Optimizer is enabling organizations to migrate from legacy port-based rules to application-based rules, which are more secure and aligned with Zero Trust principles.

Policy Optimizer identifies traffic patterns and automatically recommends the necessary application-based policies.

Why Not D:

5-tuple attributes (source IP, destination IP, source port, destination port, protocol) are used in traditional firewalls. Simplifying these attributes to 4-tuple (e.g., removing the protocol) is not a use case for Policy Optimizer, as Palo Alto Networks NGFWs focus on application-based policies, not just 5-tuple matching.

Why Not E:

Automating tagging of rules based on historical log data is not a specific feature of Policy Optimizer. While Policy Optimizer analyzes log data to recommend policy changes, tagging is not its primary use case.

Reference from Palo Alto Networks Documentation:

Policy Optimizer Overview

Transitioning to Application-Based Policies

Question 2

Question Type: MultipleChoice

Which use case is valid for Palo Alto Networks Next-Generation Firewalls (NGFWs)?

Options:

A- Code-embedded NGFWs provide enhanced internet of things (IoT) security by allowing PAN-OS code to be run on devices that do not support embedded virtual machine (VM) images.
B- Serverless NGFW code security provides public cloud security for code-only deployments that do not leverage virtual machine (VM) instances or containerized services.
C- IT/OT segmentation firewalls allow operational technology resources in plant networks to securely interface with IT resources in the corporate network.
D- PAN-OS GlobalProtect gateways allow companies to run malware and exploit prevention modules on their endpoints without installing endpoint agents.

Answer:

C

Explanation:

Palo Alto Networks Next-Generation Firewalls (NGFWs) provide robust security features across a variety of use cases. Let's analyze each option:

A . Code-embedded NGFWs provide enhanced IoT security by allowing PAN-OS code to be run on devices that do not support embedded VM images.

This statement is incorrect. NGFWs do not operate as 'code-embedded' solutions for IoT devices. Instead, they protect IoT devices through advanced threat prevention, device identification, and segmentation capabilities.

B . Serverless NGFW code security provides public cloud security for code-only deployments that do not leverage VM instances or containerized services.

This is not a valid use case. Palo Alto NGFWs provide security for public cloud environments using VM-series firewalls, CN-series (containerized firewalls), and Prisma Cloud for securing serverless architectures. NGFWs do not operate in 'code-only' environments.

C . IT/OT segmentation firewalls allow operational technology (OT) resources in plant networks to securely interface with IT resources in the corporate network.

This is a valid use case. Palo Alto NGFWs are widely used in industrial environments to provide IT/OT segmentation, ensuring that operational technology systems in plants or manufacturing facilities can securely communicate with IT networks while protecting against cross-segment threats. Features like App-ID, User-ID, and Threat Prevention are leveraged for this segmentation.

D . PAN-OS GlobalProtect gateways allow companies to run malware and exploit prevention modules on their endpoints without installing endpoint agents.

This is incorrect. GlobalProtect gateways provide secure remote access to corporate networks and extend the NGFW's threat prevention capabilities to endpoints, but endpoint agents are required to enforce malware and exploit prevention modules.

Key Takeaways:

IT/OT segmentation with NGFWs is a real and critical use case in industries like manufacturing and utilities.

The other options describe features or scenarios that are not applicable or valid for NGFWs.

Palo Alto Networks NGFW Use Cases

Industrial Security with NGFWs

Question 3

Question Type: MultipleChoice

A prospective customer is concerned about stopping data exfiltration, data infiltration, and command-and-control (C2) activities over port 53.

Which subscription(s) should the systems engineer recommend?

Options:

A- Threat Prevention
B- App-ID and Data Loss Prevention
C- DNS Security
D- Advanced Threat Prevention and Advanced URL Filtering

Answer:

C

Explanation:

DNS Security (Answer C):

DNS Security is the appropriate subscription for addressing threats over port 53.

DNS tunneling is a common method used for data exfiltration, infiltration, and C2 activities, as it allows malicious traffic to be hidden within legitimate DNS queries.

The DNS Security service applies machine learning models to analyze DNS queries in real-time, block malicious domains, and prevent tunneling activities.

It integrates seamlessly with the NGFW, ensuring advanced protection against DNS-based threats without requiring additional infrastructure.

Why Not Threat Prevention (Answer A):

Threat Prevention is critical for blocking malware, exploits, and vulnerabilities, but it does not specifically address DNS-based tunneling or C2 activities over port 53.

Why Not App-ID and Data Loss Prevention (Answer B):

While App-ID can identify applications, and Data Loss Prevention (DLP) helps prevent sensitive data leakage, neither focuses on blocking DNS tunneling or malicious activity over port 53.

Why Not Advanced Threat Prevention and Advanced URL Filtering (Answer D):

Advanced Threat Prevention and URL Filtering are excellent for broader web and network threats, but DNS tunneling specifically requires the DNS Security subscription, which specializes in DNS-layer threats.

Reference from Palo Alto Networks Documentation:

DNS Security Subscription Overview

Question 4

Question Type: MultipleChoice

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?

Options:

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.

Answer:

B

Explanation:

Segregating a network into unique BGP environments requires the ability to configure separate eBGP autonomous systems (AS) within the NGFW. Palo Alto Networks firewalls support advanced BGP features, including the ability to create and manage multiple autonomous systems.

Why 'It can be addressed by creating multiple eBGP autonomous systems' (Correct Answer B)?

PAN-OS supports the configuration of multiple eBGP AS environments. By creating unique eBGP AS numbers for different parts of the network, traffic can be segregated and routed separately. This feature is commonly used in multi-tenant environments or networks requiring logical separation for administrative or policy reasons.

Each eBGP AS can maintain its own routing policies, neighbors, and traffic segmentation.

This approach allows the NGFW to address the customer's need for segregated internal BGP environments.

Why not 'It cannot be addressed because PAN-OS does not support it' (Option A)?

This statement is incorrect because PAN-OS fully supports BGP, including eBGP, iBGP, and features like route reflectors, confederations, and autonomous systems.

Why not 'It can be addressed with BGP confederations' (Option C)?

While BGP confederations can logically group AS numbers within a single AS, they are generally used to simplify iBGP designs in very large-scale networks. They are not commonly used for segregating internal environments and are not required for the described use case.

Why not 'It cannot be addressed because BGP must be fully meshed internally to work' (Option D)?

Full mesh iBGP is only required in environments without route reflectors. The described scenario does not mention the need for iBGP full mesh; instead, it focuses on segregated environments, which can be achieved with eBGP.

Question 5

Question Type: MultipleChoice

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?

Options:

A- Yes - This is the default setting for API keys.
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 - The default setting must be changed from no limit to 120 minutes.

Answer:

D

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 the Web Interface or CLI on the firewall.

Navigate to Device > 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.

Palo Alto Networks API Documentation: https://docs.paloaltonetworks.com/apis

Configuration Guide: Managing API Key Expiration

Question 6

Question Type: MultipleChoice

A company plans to deploy identity for improved visibility and identity-based controls for least privilege access to applications and dat

a. The company does not have an on-premises Active Directory (AD) deployment, and devices are connected and managed by using a combination of Entra ID and Jamf.

Which two supported sources for identity are appropriate for this environment? (Select two.)

Options:

A- Captive portal
B- User-ID agents configured for WMI client probing
C- GlobalProtect with an internal gateway deployment
D- Cloud Identity Engine synchronized with Entra ID

Answer:

C, D

Explanation:

In this scenario, the company does not use on-premises Active Directory and manages devices with Entra ID and Jamf, which implies a cloud-native and modern management setup. Below is the evaluation of each option:

Option A: Captive portal

Captive portal is typically used in environments where identity mapping is needed for unmanaged devices or guest users. It provides a mechanism for users to authenticate themselves through a web interface.

However, in this case, the company is managing devices using Entra ID and Jamf, which means identity information can already be centralized through other means. Captive portal is not an ideal solution here.

This option is not appropriate.

Option B: User-ID agents configured for WMI client probing

WMI (Windows Management Instrumentation) client probing is a mechanism used to map IP addresses to usernames in a Windows environment. This approach is specific to on-premises Active Directory deployments and requires direct communication with Windows endpoints.

Since the company does not have an on-premises AD and is using Entra ID and Jamf, this method is not applicable.

This option is not appropriate.

Option C: GlobalProtect with an internal gateway deployment

GlobalProtect is Palo Alto Networks' VPN solution, which allows for secure remote access. It also supports identity-based mapping when deployed with internal gateways.

In this case, GlobalProtect with an internal gateway can serve as a mechanism to provide user and device visibility based on the managed devices connecting through the gateway.

This option is appropriate.

Option D: Cloud Identity Engine synchronized with Entra ID

The Cloud Identity Engine provides a cloud-based approach to synchronize identity information from identity providers like Entra ID (formerly Azure AD).

In a cloud-native environment with Entra ID and Jamf, the Cloud Identity Engine is a natural fit as it integrates seamlessly to provide identity visibility for applications and data.

This option is appropriate.

Palo Alto Networks documentation on Cloud Identity Engine

GlobalProtect configuration and use cases in Palo Alto Knowledge Base

Question 7

Question Type: MultipleChoice

Which two products can be integrated and managed by Strata Cloud Manager (SCM)? (Choose two)

Options:

A- Prisma SD-WAN
B- Prisma Cloud
C- Cortex XDR
D- VM-Series NGFW

Answer:

A, D

Explanation:

Strata Cloud Manager (SCM) is Palo Alto Networks' centralized cloud-based management platform for managing network security solutions, including Prisma Access and Prisma SD-WAN. SCM can also integrate with VM-Series firewalls for managing virtualized NGFW deployments.

Why A (Prisma SD-WAN) Is Correct

SCM is the management interface for Prisma SD-WAN, enabling centralized orchestration,

monitoring, and configuration of SD-WAN deployments.

Why D (VM-Series NGFW) Is Correct

SCM supports managing VM-Series NGFWs, providing centralized visibility and control for virtualized firewall deployments in cloud or on-premises environments.

Why Other Options Are Incorrect

B (Prisma Cloud): Prisma Cloud is a separate product for securing workloads in public cloud environments. It is not managed via SCM.

C (Cortex XDR): Cortex XDR is a platform for endpoint detection and response (EDR). It is managed through its own console, not SCM.

Palo Alto Networks Strata Cloud Manager Overview

Question 8

Question Type: MultipleChoice

According to a customer's CIO, who is upgrading PAN-OS versions, ''Finding issues and then engaging with your support people requires expertise that our operations team can better utilize elsewhere on more valuable tasks for the business.'' The upgrade project was initiated in a rush because the company did not have the appropriate tools to indicate that their current NGFWs were reaching capacity.

Which two actions by the Palo Alto Networks team offer a long-term solution for the customer? (Choose two.)

Options:

A- Recommend that the operations team use the free machine learning-powered AIOps for NGFW tool.
B- Suggest the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls.
C- Inform the CIO that the new enhanced security features they will gain from the PAN-OS upgrades will fix any future problems with upgrading and capacity.
D- Propose AIOps Premium within Strata Cloud Manager (SCM) to address the company's issues from within the existing technology.

Answer:

A, D

Explanation:

Free AIOps for NGFW Tool (Answer A):

The free AIOps for NGFW tool uses machine learning-powered analytics to monitor firewall performance, detect potential capacity issues, and provide insights for proactive management.

This tool helps operations teams identify capacity thresholds, performance bottlenecks, and configuration issues, reducing the reliance on manual expertise for routine tasks.

By using AIOps, the customer can avoid rushed upgrade projects in the future, as the tool provides predictive insights and recommendations for capacity planning.

AIOps Premium within Strata Cloud Manager (Answer D):

AIOps Premium is a paid version available within Strata Cloud Manager (SCM), offering more advanced analytics and proactive monitoring capabilities.

It helps address operational challenges by automating workflows and ensuring the health and performance of NGFWs, minimizing the need for constant manual intervention.

This aligns with the CIO's goal of freeing up the operations team for more valuable business tasks.

Why Not B:

While training may help the operations team gain confidence, the long-term focus should be on reducing their manual workload by providing automated tools like AIOps. The CIO's concern indicates that relying on manual expertise for ongoing maintenance is not a scalable solution.

Why Not C:

Simply informing the CIO about enhanced features from a PAN-OS upgrade does not address the capacity planning issues or reduce the dependency on the operations team for manual issue resolution.

Reference from Palo Alto Networks Documentation:

AIOps for NGFW Overview

Strata Cloud Manager and AIOps Integration

Question 9

Question Type: MultipleChoice

What is used to stop a DNS-based threat?

Options:

A- DNS proxy
B- Buffer overflow protection
C- DNS tunneling
D- DNS sinkholing

Answer:

D

Explanation:

DNS-based threats, such as DNS tunneling, phishing, or malware command-and-control (C2) activities, are commonly used by attackers to exfiltrate data or establish malicious communications. Palo Alto Networks firewalls provide several mechanisms to address these threats, and the correct method is DNS sinkholing.

Why 'DNS sinkholing' (Correct Answer D)?

DNS sinkholing redirects DNS queries for malicious domains to an internal or non-routable IP address, effectively preventing communication with malicious domains. When a user or endpoint tries to connect to a malicious domain, the sinkhole DNS entry ensures the traffic is blocked or routed to a controlled destination.

DNS sinkholing is especially effective for blocking malware trying to contact its C2 server or preventing data exfiltration.

Why not 'DNS proxy' (Option A)?

A DNS proxy is used to forward DNS queries from endpoints to an upstream DNS server. While it can be part of a network's DNS setup, it does not actively stop DNS-based threats.

Why not 'Buffer overflow protection' (Option B)?

Buffer overflow protection is a method used to prevent memory-related attacks, such as exploiting software vulnerabilities. It is unrelated to DNS-based threat prevention.

Why not 'DNS tunneling' (Option C)?

DNS tunneling is itself a type of DNS-based threat where attackers encode malicious traffic within DNS queries and responses. This option refers to the threat itself, not the method to stop it.

Question 10

Question Type: MultipleChoice

A prospective customer has provided specific requirements for an upcoming firewall purchase, including the need to process a minimum of 200,000 connections per second while maintaining at least 15 Gbps of throughput with App-ID and Threat Prevention enabled.

What should a systems engineer do to determine the most suitable firewall for the customer?

Options:

A- Upload 30 days of customer firewall traffic logs to the firewall calculator tool on the Palo Alto Networks support portal.
B- Download the firewall sizing tool from the Palo Alto Networks support portal.
C- Use the online product configurator tool provided on the Palo Alto Networks website.
D- Use the product selector tool available on the Palo Alto Networks website.

Answer:

B

Explanation:

Firewall Sizing Tool (Answer B):

The firewall sizing tool is the most accurate way to determine the suitable firewall model based on specific customer requirements, such as throughput, connections per second, and enabled features like App-ID and Threat Prevention.

By inputting traffic patterns, feature requirements, and performance needs, the sizing tool provides tailored recommendations.

Why Not A:

While uploading traffic logs to the calculator tool may help analyze traffic trends, it is not the primary method for determining firewall sizing.

Why Not C or D:

The product configurator tool and product selector tool are not designed for detailed performance analysis based on real-world requirements like connections per second or enabled features.

Reference from Palo Alto Networks Documentation:

Firewall Sizing Guide

P2P exams