Vendor: Palo Alto Networks

Exam Code: PSE-Strata-Pro-24

Exam Name: Palo Alto Networks Systems Engineer Professional - Hardware Firewall

Version: DEMO

QUESTION 1
A customer sees unusually high DNS traffic to an unfamiliar IP address. Which Palo Alto Networks Cloud-Delivered Security Services (CDSS) subscription should be enabled to further inspect this traffic?

A. Advanced Threat Prevention
B. Advanced WildFire
C. Advanced URL Filtering
D. Advanced DNS Security

Answer: D
Explanation:
The appropriate CDSS subscription to inspect and mitigate suspicious DNS traffic is Advanced DNS Security.

Advanced DNS Security protects against DNS-based threats, including domain generation algorithms (DGA), DNS tunneling (often used for data exfiltration), and malicious domains used in attacks. It leverages machine learning to detect and block DNS traffic associated with command-and-control servers or other malicious activities. In this case, unusually high DNS traffic to an unfamiliar IP address is likely indicative of a DNS-based attack or malware activity, making this the most suitable service.

Option D (Correct): Advanced DNS Security specifically addresses DNS-based threats. By enabling this service, the customer can detect and block DNS queries to malicious domains and investigate anomalous DNS behavior like the high traffic observed in this scenario.

QUESTION 2
While responding to a customer RFP, a systems engineer (SE) is presented the question, "How do PANW firewalls enable the mapping of transactions as part of Zero Trust principles?" Which two narratives can the SE use to respond to the question? (Choose two.)

A. Emphasize Zero Trust as an ideology, and that the customer decides how to align to Zero Trust principles.
B. Reinforce the importance of decryption and security protections to verify traffic that is not malicious.
C. Explain how the NGFW can be placed in the network so it has visibility into every traffic flow.
D. Describe how Palo Alto Networks NGFW Security policies are built by using users, applications, and data objects.

Answer: CD
Explanation:
Zero Trust is a strategic framework for securing infrastructure and data by eliminating implicit trust and continuously validating every stage of digital interaction. Palo Alto Networks NGFWs are designed with native capabilities to align with Zero Trust principles, such as monitoring transactions, validating identities, and enforcing least-privilege access. The following narratives effectively address the customer's question:

Option C (Correct): Placing the NGFW in the network provides visibility into every traffic flow across users, devices, and applications. This allows the firewall to map transactions and enforce Zero Trust principles such as segmenting networks, inspecting all traffic, and controlling access. With features like App-ID, User-ID, and Content-ID, the firewall provides granular insights into traffic flows, making it easier to identify and secure transactions.

Option D (Correct): Palo Alto Networks NGFWs use security policies based on users, applications, and data objects to align with Zero Trust principles. Instead of relying on IP addresses or ports, policies are enforced based on the application's behavior, the identity of the user, and the sensitivity of the data involved. This mapping ensures that only authorized users can access specific resources, which is a cornerstone of Zero Trust.

QUESTION 3
Which two files are used to deploy CN-Series firewalls in Kubernetes clusters? (Choose two.)

A. PAN-CN-NGFW-CONFIG
B. PAN-CN-MGMT-CONFIGMAP
C. PAN-CN-MGMT
D. PAN-CNI-MULTUS

Answer: AB
Explanation:
CN-Series firewalls are Palo Alto Networks' containerized NGFWs designed for protecting Kubernetes environments. These firewalls provide threat prevention, traffic inspection, and compliance enforcement within containerized workloads. Deploying CN-Series in a Kubernetes cluster requires specific configuration files to set up the management plane and NGFW functionalities.

Option A (Correct): PAN-CN-NGFW-CONFIG is required to define the configurations for the NGFW itself. This file contains firewall policies, application configurations, and security profiles needed to secure the Kubernetes environment.

Option B (Correct): PAN-CN-MGMT-CONFIGMAP is a ConfigMap file that contains the configuration for the management plane of the CN-Series firewall. It helps set up the connection between the management interface and the NGFW deployed within the Kubernetes cluster.

QUESTION 4
A current NGFW customer has asked a systems engineer (SE) for a way to prove to their internal management team that its NGFW follows Zero Trust principles. Which action should the SE take?

A. Use the "Monitor > PDF Reports" node to schedule a weekly email of the Zero Trust report to the internal management team.
B. Help the customer build reports that align to their Zero Trust plan in the "Monitor > Manage Custom Reports" tab.
C. Use a third-party tool to pull the NGFW Zero Trust logs, and create a report that meets the customer's needs.
D. Use the "ACC" tab to help the customer build dashboards that highlight the historical tracking of the NGFW enforcing policies.

Answer: B
Explanation:
To demonstrate compliance with Zero Trust principles, a systems engineer can leverage the rich reporting and logging capabilities of Palo Alto Networks firewalls. The focus should be on creating reports that align with the customer's Zero Trust strategy, providing detailed insights into policy enforcement, user activity, and application usage.

Option B (Correct): Custom reports in the "Monitor > Manage Custom Reports" tab allow the customer to build tailored reports that align with their Zero Trust plan. These reports can include

granular details such as application usage, user activity, policy enforcement logs, and segmentation compliance. This approach ensures the customer can present evidence directly related to their Zero Trust implementation.

QUESTION 5
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 logs.
B. Configure an NGFW as a GlobalProtect gateway, then have all users run GlobalProtect Windows SSO to gather user information.
C. Configure data redistribution to redistribute IP address-user mappings from a hub NGFW to the other spoke NGFWs.
D. Configure an NGFW as a GlobalProtect gateway, then have all users run GlobalProtect agents to gather user information.

Answer: A
Explanation:
When high traffic from Palo Alto Networks NGFWs to Active Directory servers causes performance issues, optimizing the way NGFWs gather user-to-IP mappings is critical. Palo Alto Networks offers multiple ways to collect user identity information, and Cloud Identity Engine provides a solution that reduces the load on AD servers while still ensuring efficient and accurate mapping.

Option A (Correct): Cloud Identity Engine allows NGFWs to gather user-to-IP mappings directly from Active Directory authentication logs or other identity sources without placing heavy traffic on the AD servers. By leveraging this feature, the NGFW can offload authentication-related tasks and efficiently identify users without overloading AD servers. This solution is scalable and minimizes the overhead typically caused by frequent User-ID queries to AD servers.

QUESTION 6
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.

Answer: B
Explanation:
When preparing for a customer meeting, it's important to understand their specific challenges and align solutions accordingly. The notes suggest that the customer is facing difficulties securing

their cloud apps and remote users, which are core areas addressed by Palo Alto Networks' Zero Trust and SASE solutions. However, jumping directly into a pitch or product demonstration without validating the customer's specific challenges may fail to build trust or fully address their needs.

Option B (Correct): Discovery questions are a critical step in the sales process, especially when addressing complex topics like Zero Trust. By designing targeted questions about the customer's challenges with identity, devices, data, and access, the SE can identify specific pain points. These insights can then be used to tailor a Zero Trust strategy that directly addresses the customer's concerns. This approach ensures the meeting is customer-focused and demonstrates that the SE understands their unique needs.

QUESTION 7
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.)

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: AD
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.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**