Palo Alto PSE Strata Professional Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What is a platform component use of the Cortex Data Lake?

A. Cortex XDR Prevent receives data from the Cortex Data Lake to do its zero-day attack analysis.

B. Cortex XDR provides data to the Cortex Data Lake after applying AI and machine learning to firewall and other sensor traffic.

C. Prisma Access extracts data from the Cortex Data Lake to help inform CASB proxy functionality for tolerated SaaS applications.

D. Third-party applications make use of data in the Cortex Data Lake.

2. Which fully populated firewall has the highest file forwarding capacity?

A. PA-200

B. PA-5280

C. VM-100

D. PA-7080

3. Which component is essential for managing user identity information within Palo Alto firewalls?

A. Security Zones

B. User-ID agent

C. Management Interface

D. Traffic Logs

4. What type of appliances can the WildFire service use for protection without internet connection?

A. WF-400 appliance

B. WF-500 appliance

C. WF-600 appliance

D. No appliance is necessary

5. How does buying 5 new domain names each week for C2 affect a botnet report?

- **A. It helps disguise the malware.**
- **B. Access to new domains (registered in the last week) is counted as suspicious.**
- **C. Access to new domains (registered in the last 30 days) is counted as suspicious.**
- **D. Access to new domains (registered in the last 60 days) is counted as suspicious.**

6. What is the primary purpose of BPA with Heatmaps?

- **A. To assess deployment progress**
- **B. To analyze network threats**
- **C. To provide quality assurance measures**
- **D. To evaluate applications running on the network**

7. How does the next-generation firewall (NGFW) fit into the Palo Alto Networks SaaS security solution?

- **A. It is replaced by Prisma Access.**
- **B. It provides inline security.**
- **C. Its functionality is superseded by the CASB proxy.**
- **D. It offers the same security for in-house apps that Prisma SaaS provides for SaaS apps.**

8. Which elements are included in a "Security Incident" report generated by Palo Alto Networks tools?

- **A. Details such as the source of traffic and time of incident**
- **B. Details such as who initiated the traffic and actions taken**
- **C. Details about network topology and device settings**
- **D. Details including user credentials and personal data**

9. How do Quality of Service (QoS) policies contribute to network performance?

- **A. By limiting the number of devices connected**
- **B. By prioritizing critical traffic over less important traffic**
- **C. By encrypting all data packets**
- **D. By automatically updating bandwidth policies**

10. How does "IPsec VPN" function within Palo Alto Networks devices?

A. It compresses data for faster transmission.

B. It creates secure tunnels for encrypted communications.

C. It monitors traffic for unusual behavior.

D. It separates traffic based on application type.

Answers

1. A
2. D
3. B
4. B
5. C
6. A
7. B
8. B
9. B
10. B

Explanations

1. What is a platform component use of the Cortex Data Lake?

A. Cortex XDR Prevent receives data from the Cortex Data Lake to do its zero-day attack analysis.

B. Cortex XDR provides data to the Cortex Data Lake after applying AI and machine learning to firewall and other sensor traffic.

C. Prisma Access extracts data from the Cortex Data Lake to help inform CASB proxy functionality for tolerated SaaS applications.

D. Third-party applications make use of data in the Cortex Data Lake.

The correct choice highlights a specific use case of the Cortex Data Lake where Cortex XDR Prevent leverages the data stored within the Lake to conduct analysis, particularly for detecting zero-day attacks. The Cortex Data Lake functions as a robust centralized repository for data collected from various sources, including security events and logs from different products. Cortex XDR Prevent uses this comprehensive data analysis to enhance threat detection capabilities. When it refers to zero-day attacks, it indicates the ability of the Cortex XDR to analyze incoming data to identify threats that exploit vulnerabilities not yet known to security teams. This illustrates the Cortex Data Lake's role in supporting advanced security functions, allowing proactive measures against sophisticated and unknown threats. In contrast, the other options provide insights into different interactions with the Cortex Data Lake, but they do not specifically point to the analysis of zero-day threats by the Cortex XDR Prevent as the selected choice does. This clarification helps to understand the specific functionality and application of data within the ecosystem of Palo Alto Networks' security architecture.

2. Which fully populated firewall has the highest file forwarding capacity?

A. PA-200

B. PA-5280

C. VM-100

D. PA-7080

The PA-7080 is recognized for having the highest file forwarding capacity among the options provided. This capability is primarily due to its advanced hardware architecture, which is designed to handle a significant volume of network traffic with reduced latency. The PA-7080 features high-performance processing components and enhanced memory specifications that allow it to support a larger number of policies and sessions simultaneously. Furthermore, the PA-7080 utilizes advanced integrated features such as application identification, intrusion prevention, and URL filtering at high speeds, maximizing its operational efficiency. This ensures that as the demand for bandwidth increases, the PA-7080 can maintain performance standards without compromising security features. Other models, such as the PA-200, PA-5280, and VM-100, while capable in their own right, do not match the PA-7080's specifications and performance capabilities, particularly in high-throughput environments. Thus, for organizations requiring a robust firewall solution to manage extensive data flows, the PA-7080 stands out as the optimal choice.

3. Which component is essential for managing user identity information within Palo Alto firewalls?

A. Security Zones

B. User-ID agent

C. Management Interface

D. Traffic Logs

The User-ID agent is essential for managing user identity information within Palo Alto firewalls because it serves as the bridge between the firewall and the user directory, such as Active Directory. This agent allows for the identification and mapping of users to their respective IP addresses, enabling the firewall to enforce security policies based on user identity rather than just IP addresses. This capability is crucial for implementing user-based policies, providing visibility into user activities, and ensuring that security measures are accurately applied based on who is accessing the network. While the other components listed have their own important roles—security zones primarily classify and control traffic, the management interface provides a way to configure and manage the firewall, and traffic logs track and record session data—they do not specifically focus on managing and mapping user identity, which is a vital aspect of user-based policy enforcement within the Palo Alto environment.

4. What type of appliances can the WildFire service use for protection without internet connection?

A. WF-400 appliance

B. WF-500 appliance

C. WF-600 appliance

D. No appliance is necessary

The WF-500 appliance is designed to operate effectively in environments where an internet connection may not be available, providing crucial protections against malware and other threats. This model is equipped with advanced capabilities for detecting and blocking malicious traffic and can process data locally, ensuring that organizations can maintain security measures even in isolated or offline scenarios. The need for an appliance with these capabilities is critical in environments where reliable internet access cannot be guaranteed, allowing organizations to continue safeguarding their digital infrastructure without interruption. The WF-500 supports various features designed to enhance protection and maintain functionality in a variety of operational situations.

5. How does buying 5 new domain names each week for C2 affect a botnet report?

A. It helps disguise the malware.

B. Access to new domains (registered in the last week) is counted as suspicious.

C. Access to new domains (registered in the last 30 days) is counted as suspicious.

D. Access to new domains (registered in the last 60 days) is counted as suspicious.

Buying 5 new domain names each week for command and control (C2) purposes plays a crucial role in the operational security of a botnet. When malware communicates with its C2 servers, it often utilizes these domains to connect and receive instructions. The focus on new domain names is particularly significant because these domains may not have been fully vetted by security measures or blacklists yet, thus potentially offering a means to evade detection. When it comes to botnet reports, particularly in regard to identifying suspicious activity, the timeframe for counting newly registered domains is key. Access to new domains registered within the last 30 days is often concerning for security analysts because it indicates active threats that could be continuously evolving. Analysts regularly flag these domains as suspicious, as they may be indicative of malicious activity such as botnets trying to avoid exposure by constantly shifting their C2 infrastructure. This awareness allows security operations to monitor and respond to these domains effectively, strengthening systems and methodologies for identifying and mitigating threats. In contrast, the other timeframes specified, such as 60 days or longer, may not offer the same immediacy of threat and would typically not be flagged in the same way, as the domains would potentially have been categorized and evaluated longer, reducing the likelihood of

6. What is the primary purpose of BPA with Heatmaps?

A. To assess deployment progress

B. To analyze network threats

C. To provide quality assurance measures

D. To evaluate applications running on the network

The primary purpose of Business Process Analysis (BPA) with Heatmaps is to assess deployment progress. Heatmaps are visualization tools that represent data in a way that is easy to understand at a glance. In the context of BPA, these heatmaps can display various metrics related to deployment, such as the status of processes, the effectiveness of specific functions, and areas that may require attention. This assessment helps organizations identify areas of improvement in their deployment strategies, enabling them to optimize performance and enhance productivity. While evaluating applications running on the network, analyzing network threats, and providing quality assurance measures are important aspects of IT governance and management, they do not align as directly with the fundamental goal of BPA when used with heatmaps. BPA's focus is on understanding and improving business processes, and heatmaps serve as a valuable tool to visually track and assess how well those processes are being deployed within an organization.

7. How does the next-generation firewall (NGFW) fit into the Palo Alto Networks SaaS security solution?

A. It is replaced by Prisma Access.

B. It provides inline security.

C. Its functionality is superseded by the CASB proxy.

D. It offers the same security for in-house apps that Prisma SaaS provides for SaaS apps.

The next-generation firewall (NGFW) plays a crucial role in the Palo Alto Networks SaaS security solution by providing inline security. This means that the NGFW actively inspects and controls the data traffic as it flows through the network, allowing for real-time threat detection and response. This is vital for organizations as it enhances overall security posture by integrating various security features such as application visibility, user identification, and advanced threat protection into the network traffic flow. The inline capability of the NGFW enables it to enforce security policies on the fly, ensuring that malicious content is blocked and users are protected while accessing SaaS applications or any other network resources. This functionality is foundational for a comprehensive security strategy that encompasses both traditional on-premise infrastructure and modern cloud services, enabling seamless security across diverse environments. While other solutions like Prisma Access and CASB (Cloud Access Security Broker) provide valuable security features, the NGFW remains an integral part of the security architecture, particularly for organizations requiring robust, inline security for all types of applications, whether they are on-premise or in the cloud.

8. Which elements are included in a "Security Incident" report generated by Palo Alto Networks tools?

A. Details such as the source of traffic and time of incident

B. Details such as who initiated the traffic and actions taken

C. Details about network topology and device settings

D. Details including user credentials and personal data

A "Security Incident" report generated by Palo Alto Networks tools typically includes critical information about the incident's context and response, which is why the details about who initiated the traffic and actions taken are essential components. These elements help security teams understand not just what happened during a specific incident, but also who was involved and what measures were taken in response. Knowing who initiated the traffic assists in identifying potential insider threats or accidental misconfigurations, while the actions taken indicate the effectiveness of the organization's incident response plan. This information is vital for post-incident analysis and can guide future security procedures and policies. In contrast, while details like the source of traffic and time of incident are important for overall situational awareness, they do not provide the same depth of insight into the response actions or the actors involved. Similarly, information about network topology and device settings, as well as user credentials and personal data, may not be relevant in the context of understanding the specific incident and response.

9. How do Quality of Service (QoS) policies contribute to network performance?

A. By limiting the number of devices connected

B. By prioritizing critical traffic over less important traffic

C. By encrypting all data packets

D. By automatically updating bandwidth policies

Quality of Service (QoS) policies play a significant role in enhancing network performance by prioritizing critical traffic over less important traffic. This prioritization ensures that bandwidth and network resources are allocated efficiently, allowing essential applications and services—such as VoIP, video conferencing, and critical business applications—to function optimally even during peak usage times. When traffic is prioritized, QoS mechanisms can adjust the flow of data, reducing latency and jitter for high-priority traffic while allowing less important traffic to be transmitted at a lower priority. This is crucial in maintaining the quality of user experiences, especially in environments where network congestion might occur. As a direct result, applications that require timely data delivery benefit the most from QoS implementations, leading to improved overall network performance and reliability. Other options, while they might have relevance in broader aspects of networking, do not directly address the specific role that QoS policies play in enhancing performance through traffic prioritization.

10. How does "IPsec VPN" function within Palo Alto Networks devices?

A. It compresses data for faster transmission.

B. It creates secure tunnels for encrypted communications.

C. It monitors traffic for unusual behavior.

D. It separates traffic based on application type.

IPsec VPN functions by creating secure tunnels for encrypted communications. This technology is integral to networking, especially when it comes to ensuring that the data transmitted over untrusted networks, such as the Internet, remains confidential and secure. When using IPsec VPN, Palo Alto Networks devices encapsulate and encrypt the data packets that are sent between two endpoints. This means that even if the data is intercepted in transit, it cannot be deciphered by unauthorized parties. The secure tunnels are established using a series of protocols that handle authentication, encryption, and key exchange, ensuring that only legitimate users can access the data stream. This is particularly important for organizations that need to protect sensitive information, facilitate secure remote access for employees, or connect multiple branch offices securely. Without the secure tunnel created by IPsec, data could be vulnerable to eavesdropping and tampering, undermining the organization's security posture. In contrast, compression of data, monitoring for unusual behavior, or separating traffic based on application type do not characterize the primary function of IPsec VPNs. While those features are important in various contexts of network management and security, they do not describe the core purpose of IPsec VPN technology itself.