Free Questions for PSE-SoftwareFirewall by certscare

Shared by Freeman on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which component scans for threats in allowed traffic?

Options:

A- Security profiles

B- NAT

C- Intelligent Traffic Offload

D- TLS decryption

Answer:

A

Explanation:

Security Profiles:

Security profiles in Palo Alto Networks firewalls are used to scan for threats in allowed traffic. These profiles include features such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, and others that inspect traffic and detect potential threats.

Palo Alto Networks Security Profiles

Question 2

Question Type: MultipleChoice

How does Prisma Cloud Compute offer workload security at runtime?

Options:

A- It quarantines containers that demonstrate increased CPU and memory usage.

B- It automatically patches vulnerabilities and compliance issues for every container and service.

C- It works with the identity provider (IdP) to identify overprivileged containers and services, and it restricts network access.

D- It automatically builds an allow-list security model for every container and service.

Answer:

D

Explanation:

Allow-list Security Model:

Prisma Cloud Compute provides runtime security by automatically creating an allow-list security model for each container and service. This model ensures that only expected and authorized behaviors are allowed, effectively preventing unauthorized activities.

Prisma Cloud Compute Runtime Security

Question 3

Question Type: MultipleChoice

What is a benefit of network runtime security?

Options:

A- It removes vulnerabilities that have been baked into containers.

B- It more narrowly focuses on one security area and requires careful customization, integration, and maintenance.

C- It is siloed to enhance workload security.

D- It identifies unknown vulnerabilities that cannot be identified by known Common Vulnerability and Exposure (CVE) lists.

Answer:

D

Explanation:

Identifying Unknown Vulnerabilities:

Network runtime security is beneficial because it can identify unknown vulnerabilities that are not listed in known CVE lists. This type of security focuses on monitoring the behavior of applications and containers in real-time, which helps detect anomalies and potential threats that static analysis might miss.

Palo Alto Networks Runtime Security Guide

Question 4

Question Type: MultipleChoice

What are two requirements for automating service deployment of a VM-Series firewall from an NSX Manager? (Choose two.)

Options:

A- Panorama has been configured to recognize both the NSX Manager and vCenter.

B- vCenter has been given Palo Alto Networks subscription licenses for VM-Series firewalls.

C- The deployed VM-Series firewall can establish communications with Panorama.

D- Panorama can establish communications to the public Palo Alto Networks update servers.

Answer:

A, C

Explanation:

For automating the deployment of VM-Series firewalls from NSX Manager, Panorama must be configured to recognize and communicate with both the NSX Manager and vCenter. This ensures that Panorama can manage the firewall policies and orchestration efficiently.

Palo Alto Networks NSX Integration Guide

VM-Series Firewall Communication with Panorama:

It is crucial that the deployed VM-Series firewall can establish communication with Panorama. This connection allows for the centralized management of the firewalls and ensures that policy updates and configurations can be pushed from Panorama to the VM-Series firewalls.

Palo Alto Networks VM-Series Deployment Guide

Question 5

Question Type: MultipleChoice

Which component can provide application-based segmentation and prevent lateral threat movement?

Options:

A- DNS Security

B- NAT

C- App-ID *

D- URL Filtering

Answer:

C

Explanation:

App-ID is a feature that provides application-based segmentation and helps prevent lateral threat movement within a network. By identifying and controlling applications traversing the network regardless of port, protocol, or encryption (SSL or SSH), App-ID allows granular security policies to be applied, thereby limiting the spread of threats within the network.

Palo Alto Networks App-ID Technology: App-ID

Palo Alto Networks Application and Threat Content: App-ID Overview

Question 6

Question Type: MultipleChoice

When implementing active-active high availability (HA), which feature must be configured to allow the HA pair to share a single IP address that may be used as the network's gateway IP address?

Options:

A- Floating IP address

B- VRRP

C- ARP load sharing

D- HSRP

Answer:

A

Explanation:

When implementing active-active high availability (HA), a floating IP address must be configured to allow the HA pair to share a single IP address that may be used as the network's gateway IP address. This floating IP address ensures that either of the active-active firewalls can assume control of the traffic without interruption in case of a failover.

Palo Alto Networks High Availability Guide: Active-Active HA Configuration

Palo Alto Networks HA Configuration: HA Configuration

Question 7

Question Type: **MultipleChoice**

Which offering inspects encrypted outbound traffic?

Options:

A- TLS decryption

B- Content-ID

C- Advanced URL Filtering (AURLF)

D- WildFire

Answer:

A

Explanation:

TLS decryption is the feature that inspects encrypted outbound traffic. By decrypting TLS/SSL traffic, the firewall can inspect the content for threats and enforce security policies. This is crucial for preventing malware and other threats that might hide within encrypted traffic.

Palo Alto Networks TLS Decryption Documentation: TLS Decryption