Palo Alto Networks

PCSFE Exam

Palo Alto Networks Certified Software Firewall Engineer

Questions & Answers
Demo

Version: 4.0

Question: 1

Which two subscriptions should be recommended to a customer who is deploying VM-Series firewalls to a private data center but is concerned about protecting data-center resources from malware and lateral movement? (Choose two.)

A. Intelligent Traffic Offload
B. Threat Prevention
C. WildFire
D. SD-WAN

Answer: B, C

Explanation:

Threat Prevention and WildFire are the two subscriptions that provide protection against malware and lateral movement in a private data center. Threat Prevention blocks known threats using antivirus, anti-spyware, and vulnerability protection. WildFire analyzes unknown files and links in a cloud-based sandbox and generates signatures for new threats. Intelligent Traffic Offload is a feature that reduces the load on the firewall by offloading traffic that does not need inspection. SD-WAN is a feature that optimizes the performance and availability of WAN connections. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Threat Prevention Datasheet], [WildFire Datasheet], [Intelligent Traffic Offload], [SD-WAN]

Question: 2

Which two mechanisms could trigger a high availability (HA) failover event? (Choose two.)

A. Heartbeat polling
B. Ping monitoring
C. Session polling
D. Link monitoring

Answer: A, D

Explanation:

Heartbeat polling and link monitoring are two mechanisms that can trigger an HA failover event. Heartbeat polling is a method of verifying the health of the peer firewall by sending periodic heartbeat messages. If the heartbeat messages are not received within a specified interval, the firewall assumes that the peer is down and initiates a failover. Link monitoring is a method of verifying the connectivity of the interfaces on the firewall by sending link state packets. If the link

state packets are not received on a specified number of interfaces, the firewall assumes that the network is down and initiates a failover. Ping monitoring and session polling are not HA mechanisms, but they are used for path monitoring and session synchronization respectively. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [High Availability Overview], [Configure HA Link Monitoring], [Configure HA Path Monitoring], [Configure Session Synchronization]

Question: 3

Which technology allows for granular control of east-west traffic in a software-defined network?

A. Routing
B. Microseqmentation
C. MAC Access Control List
D. Virtualization

Answer: B

Explanation:

Microsegmentation is a technology that allows for granular control of east-west traffic in a software-defined network. Microsegmentation divides the network into smaller segments or zones based on application or workload characteristics, and applies security policies to each segment. This reduces the attack surface and prevents unauthorized access or lateral movement within the network. Routing, MAC Access Control List, and Virtualization are not technologies that provide microsegmentation, but they are related concepts that can be used in conjunction with microsegmentation. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Microsegmentation with Palo Alto Networks], [Microsegmentation for Dummies]

Question: 4

Which solution is best for securing an EKS environment?

A. VM-Series single host
B. CN-Series high availability (HA) pair
C. PA-Series using load sharing
D. API orchestration

Answer: B

Explanation:

CN-Series high availability (HA) pair is the best solution for securing an EKS environment. EKS is a managed service that allows users to run Kubernetes clusters on AWS. CN-Series is a containerized firewall that integrates with Kubernetes and provides visibility and control over container traffic. CN-Series HA pair consists of two CN-Series firewalls deployed in active-passive mode to provide redundancy and failover protection. VM-Series single host, PA-Series using load sharing, and API orchestration are not optimal solutions for securing an EKS environment, as they do not offer the same level of integration, scalability, and automation as CN-Series. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Deployment Guide for AWS EKS], [CN-Series

Datasheet]

Question: 5

A CN-Series firewall can secure traffic between which elements?

A. Host containers
B. Source applications
C. Containers
D. IPods

Answer: C

Explanation:

Containers are the elements that a CN-Series firewall can secure traffic between. Containers are isolated units of software that run on a shared operating system and have their own resources, dependencies, and configuration. A CN-Series firewall can inspect and enforce security policies on traffic between containers within a pod, across pods, or across namespaces in a Kubernetes cluster. Host containers, source applications, and IPods are not valid elements that a CN-Series firewall can secure traffic between. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Concepts], [What is a Container?]