PCSFE$^{\text{Q\&As}}$

Palo Alto Networks Certified Software Firewall Engineer (PCSFE)

Pass Palo Alto Networks PCSFE Exam with 100% Guarantee

QUESTION 1

Why are containers uniquely suitable for runtime security based on allow lists?

A. Containers have only a few defined processes that should ever be executed.

B. Developers define the processes used in containers within the Dockerfile.

C. Docker has a built-in runtime analysis capability to aid in allow listing.

D. Operations teams know which processes are used within a container.

Correct Answer: A

Explanation: Containers are uniquely suitable for runtime security based on allow lists because containers have only a few defined processes that should ever be executed. Developers can specify the processes that are allowed to run in a container using a Dockerfile, but this does not guarantee that only those processes will run at runtime. Therefore, using an allow list approach can prevent any unauthorized or malicious processes from running in a container2. References: Container Security

QUESTION 2

What is a design consideration for a prospect who wants to deploy VM-Series firewalls in an Amazon Web Services (AWS) environment?

A. Special AWS plugins are needed for load balancing.

B. Resources are shared within the cluster.

C. Only active-passive high availability (HA) is supported.

D. High availability (HA) clusters are limited to fewer than 8 virtual appliances.

Correct Answer: C

Explanation: A design consideration for a prospect who wants to deploy VM-Series firewalls in an Amazon Web Services (AWS) environment is that only active-passive high availability (HA) is supported. High availability (HA) is a feature that provides redundancy and failover protection for firewalls in case of hardware or software failure. Active-passive HA is a mode of HA that consists of two firewalls in a pair, where one firewall is active and handles all traffic, while the other firewall is passive and acts as a backup. Active-passive HA is the only mode of HA that is supported for VM-Series firewalls in an AWS environment, due to the limitations of AWS networking and routing. Active-active HA, which is another mode of HA that consists of two firewalls in a pair that both handle traffic and synchronize sessions, is not supported for VM-Series firewalls in an AWS environment. A design consideration for a prospect who wants to deploy VM-Series firewalls in an AWS environment is not that special AWS plugins are needed for load balancing, resources are shared within the cluster, or high availability (HA) clusters are limited to fewer than 8 virtual appliances, as those are not valid or relevant factors for firewall deployment in an AWS environment. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [High Availability Overview], [High Availability on AWS]

QUESTION 3

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

Correct Answer: AD

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. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [High Availability Overview], [Configure HA Link Monitoring], [Configure HA Path Monitoring], [Configure Session Synchronization]

QUESTION 4

What is a benefit of network runtime security?

A. It more narrowly focuses on one security area and requires careful customization integration and maintenance

B. It removes vulnerabilities that have been baked into containers.

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.

Correct Answer: D

Explanation: A benefit of network runtime security is that it identifies unknown vulnerabilities that cannot be identified by known Common Vulnerability and Exposure (CVE) lists. Network runtime security is a type of security that monitors and analyzes network traffic in real time to detect and prevent malicious activities or anomalous behaviors. Network runtime security can identify unknown vulnerabilities that cannot be identified by known CVE lists, such as zero-day exploits, advanced persistent threats, or custom malware. Network runtime security can also provide visibility and context into network activity, such as application dependencies, user identities, device types, or threat intelligence. Network runtime security does not more narrowly focus on one security area and requires careful customization, integration, and maintenance, remove vulnerabilities that have been baked into containers, or is siloed to enhance workload security, as those are not benefits or characteristics of network runtime security. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Network Runtime Security], [What is CVE?]

QUESTION 5

What can software next-generation firewall (NGFW) credits be used to provision?

A. Remote browser isolation

B. Virtual Panorama appliances

C. Migrating NGFWs from hardware to VMs

D. Enablement of DNS security

Correct Answer: C

Explanation: Software next-generation firewall (NGFW) credits can be used to provision migrating NGFWs from hardware to VMs. Software NGFW credits are a flexible licensing model that allows customers to purchase and consume software NGFWs as needed, without having to specify the platform or deployment model upfront. Customers can use software NGFW credits to migrate their existing hardware NGFWs to VM-Series firewalls on any supported cloud or virtualization platform, or to deploy new VM-Series firewalls as their needs grow. Software NGFW credits cannot be used to provision remote browser isolation, virtual Panorama appliances, or enablement of DNS security, as those are separate solutions that require different licenses or subscriptions. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Software NGFW Credits Datasheet], [Software NGFW Credits FAQ]