Free Questions for PCSFE by braindumpscollection

Shared by Cannon on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Why are VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster problematic for protecting containerized workloads?

Options:

A- They are located outside the cluster and have no visibility into application-level cluster traffic.

B- They do not scale independently of the Kubernetes cluster.

C- They are managed by another entity when located inside the cluster.

D- They function differently based on whether they are located inside or outside of the cluster.

Answer:

A

Explanation:

VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster are problematic for protecting containerized workloads because they are located outside the cluster and have no visibility into application-level cluster traffic. Kubernetes is a platform that provides orchestration, automation, and management of containerized applications. Kubernetes cluster traffic consists of traffic between containers within a pod, across pods, or across namespaces. VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster cannot inspect or control this traffic, as they only see the encapsulated or aggregated traffic at the network layer. This creates blind spots and security gaps for containerized workloads. VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster are not problematic for protecting containerized workloads because they do not scale independently of the Kubernetes cluster, are managed by another entity when located inside the cluster, or function differently based on whether they are located inside or outside of the cluster, as those are not valid reasons or scenarios for firewall deployment in a Kubernetes environment. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Concepts], [VM-Series on Kubernetes]

Question 2

Question Type: **MultipleChoice**

What are two environments supported by the CN-Series firewall? (Choose two.)

Options:

A- Positive K

B- OpenShift

C- OpenStack

D- Native K8

Answer:

B, D

Explanation:

The two environments supported by the CN-Series firewall are:

OpenShift

Native K8

The CN-Series firewall is a containerized firewall that integrates with Kubernetes and provides visibility and control over container traffic. The CN-Series firewall can be deployed in various environments that support Kubernetes, such as public clouds, private clouds, or on-premises data centers. OpenShift is an environment supported by the CN-Series firewall. OpenShift is a platform that provides enterprise-grade Kubernetes and container orchestration, as well as developer tools and services. Native K8 is an environment supported by the CN-Series firewall. Native K8 is a term that refers to the standard Kubernetes distribution that is available from the Kubernetes project website, without any vendor-specific modifications or additions. Positive K and OpenStack are not environments supported by the CN-Series firewall, but they are related concepts that can be used for other purposes. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Datasheet], [CN-Series Deployment Guide for OpenShift], [CN-Series Deployment Guide for Native K8], [What is OpenShift?], [What is Kubernetes?]

Question 3

Question Type: MultipleChoice

Which two actions can be performed for VM-Series firewall licensing by an orchestration system? (Choose two.)

Options:

A- Creating a license

B- Renewing a license

C- Registering an authorization code

D- Downloading a content update

Answer:

A, C

Explanation:

The two actions that can be performed for VM-Series firewall licensing by an orchestration system are:

Creating a license

Registering an authorization code

An orchestration system is a software tool that automates and coordinates complex tasks across multiple devices or platforms. An orchestration system can perform various actions for VM-Series firewall licensing by using the Palo Alto Networks Licensing API. The Licensing API is a RESTful API that allows programmatic control of license management for VM-Series firewalls. Creating a license is an action that can be performed for VM-Series firewall licensing by an orchestration system using the Licensing API. Creating a license involves generating a license key for a VM-Series firewall based on its CPU ID and the license type. Registering an authorization code is an action that can be performed for VM-Series firewall licensing by an orchestration system using the Licensing API. Registering an authorization code involves activating a license entitlement for a VM-Series firewall based on its authorization code and CPU ID. Renewing a license and downloading a content update are not actions that can be performed for VM-Series firewall licensing by an orchestration system using the Licensing API, but they are related tasks that can be done manually or through other methods. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Licensing API Overview], [Licensing API Reference Guide]

Question 4

Question Type: **MultipleChoice**

Which two methods of Zero Trust implementation can benefit an organization? (Choose two.)

Options:

A- Compliance is validated.

B- Boundaries are established.

C- Security automation is seamlessly integrated.

D- Access controls are enforced.

Answer:

B, D

Explanation:

The two methods of Zero Trust implementation that can benefit an organization are:

Boundaries are established

Access controls are enforced

Zero Trust is a security model that assumes no trust for any entity or network segment, and requires continuous verification and validation of all connections and transactions. Zero Trust implementation can benefit an organization by improving its security posture, reducing its attack surface, and enhancing its visibility and compliance. Boundaries are established is a method of Zero Trust implementation that involves defining and segmenting the network into smaller zones based on data sensitivity, user identity, device type, or application function. Boundaries are established can benefit an organization by isolating and protecting critical assets from unauthorized access or lateral movement. Access controls are enforced is a method of Zero Trust implementation that involves applying granular security policies based on the principle of least privilege to each zone or connection. Access controls are enforced can benefit an organization by preventing data exfiltration, malware propagation, or credential theft. Compliance is validated and security automation is seamlessly integrated are not methods of Zero Trust implementation, but they may be potential outcomes or benefits of implementing Zero Trust. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Zero Trust Security Model], [Zero Trust Network Security]

Question 5

Question Type: MultipleChoice

What do tags allow a VM-Series firewall to do in a virtual environment?

Options:

A- Enable machine learning (ML).

B- Adapt Security policy rules dynamically.

C- Integrate with security information and event management (SIEM) solutions.

D- Provide adaptive reporting.

Answer:

B

Explanation:

Tags allow a VM-Series firewall to adapt Security policy rules dynamically in a virtual environment. Tags are labels or identifiers that can be assigned to virtual machines (VMs), containers, or other resources in a virtual environment. Tags can be used to group resources based on various criteria, such as application, function, location, owner, or security posture. A VM-Series firewall can leverage tags to populate Dynamic Address Groups and update Security policies accordingly, without requiring manual changes. Tags do not enable machine learning (ML), integrate with security information and event management (SIEM) solutions, or provide adaptive reporting, but they are related features that can enhance security and visibility. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Tagging Overview], [Dynamic Address Groups Overview]

Question 6

Question Type: MultipleChoice

What Palo Alto Networks software firewall protects Amazon Web Services (AWS) deployments with network security delivered as a managed cloud service?

Options:

A- VM-Series

B- Cloud next-generation firewall

C- CN-Series

D- Ion-Series Ion-Series

Answer:

B

Explanation:

Cloud next-generation firewall is the Palo Alto Networks software firewall that protects Amazon Web Services (AWS) deployments with network security delivered as a managed cloud service. Cloud next-generation firewall is a cloud-native solution that provides comprehensive security and visibility across AWS environments, including VPCs, regions, accounts, and workloads. Cloud next-generation firewall is deployed and managed by Palo Alto Networks as a service, eliminating the need for customers to provision, configure, or maintain any infrastructure or software. VM-Series, CN-Series, and Ion-Series are not Palo Alto Networks software firewalls that protect AWS deployments with network security delivered as a managed cloud service, but they are related solutions that can be deployed on AWS or other platforms. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Cloud Next-Generation Firewall Datasheet], [VM-Series Datasheet], [CN-Series Datasheet], [Ion-Series Datasheet]

Question 7

Question Type: MultipleChoice

Auto scaling templates for which type of firewall enable deployment of a single auto scaling group (ASG) of VM-Series firewalls to secure inbound traffic from the internet to Amazon Web Services (AWS) application workloads?

Options:

A- HA-Series

B- CN-Series

C- IPA-Series

D- VM-Series

Answer:

D

Explanation:

Auto scaling templates for VM-Series firewalls enable deployment of a single auto scaling group (ASG) of VM-Series firewalls to secure inbound traffic from the internet to Amazon Web Services (AWS) application workloads. An ASG is a collection of EC2 instances that

share similar characteristics and can be scaled up or down automatically based on demand or predefined conditions. Auto scaling templates for VM-Series firewalls are preconfigured templates that provide the necessary resources and configuration to deploy and manage VM-Series firewalls in an ASG on AWS. Auto scaling templates for VM-Series firewalls can be used to secure inbound traffic from the internet to AWS application workloads by placing the ASG of VM-Series firewalls behind an AWS Application Load Balancer (ALB) or a Gateway Load Balancer (GWLB) that distributes the traffic across the firewalls. The firewalls can then inspect and enforce security policies on the inbound traffic before sending it to the application workloads. Auto scaling templates for HA-Series, CN-Series, and IPA-Series firewalls do not enable deployment of a single ASG of VM-Series firewalls to secure inbound traffic from the internet to AWS application workloads, as those are different types of firewalls that have different deployment models and use cases.
Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Auto Scaling the VM-Series Firewall on AWS], [VM-Series Datasheet], [HA-Series Datasheet], [CN-Series Datasheet], [IPA-Series Datasheet]

Question 8

Question Type: **MultipleChoice**

Which two factors lead to improved return on investment for prospects interested in Palo Alto Networks virtualized next-generation firewalls (NGFWs)? (Choose two.)

Options:

A- Decreased likelihood of data breach

B- Reduced operational expenditures

C- Reduced time to deploy

D- Reduced insurance premiums

Answer:

A, C

Explanation:

The two factors that lead to improved return on investment for prospects interested in Palo Alto Networks virtualized next-generation firewalls (NGFWs) are:

Decreased likelihood of data breach

Reduced time to deploy

Palo Alto Networks virtualized NGFWs are virtualized versions of the Palo Alto Networks next-generation firewall that can be deployed on various cloud or virtualization platforms. Palo Alto Networks virtualized NGFWs provide comprehensive security and visibility across hybrid and multi-cloud environments, protecting applications and data from cyberattacks. By using Palo Alto Networks virtualized NGFWs, prospects can decrease the likelihood of data breach by applying granular security policies based on application, user, content, and threat information, and by leveraging cloud-delivered services such as Threat Prevention, WildFire, URL Filtering, DNS Security, and Cortex Data Lake. By using Palo Alto Networks virtualized NGFWs, prospects can also reduce the time to deploy by taking advantage of automation and orchestration tools such as Terraform, Ansible, CloudFormation, ARM templates, and Panorama plugins that simplify and accelerate the deployment and configuration of firewalls across different cloud platforms. Reduced operational expenditures and reduced insurance premiums are not factors that lead to improved return on investment for prospects interested in Palo Alto Networks virtualized NGFWs, but they may be potential benefits or outcomes of using them. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [VM-Series Datasheet], [CN-Series Datasheet], [Cloud Security Solutions]