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

Palo Alto Networks Certified Software Firewall Engineer (PCSFE)

Pass Palo Alto Networks PCSFE Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/pcsfe.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

QUESTION 1

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

A. Creating a license

B. Renewing a license

C. Registering an authorization code

D. Downloading a content update

Correct Answer: AC

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. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Licensing API Overview], [Licensing API Reference Guide]

QUESTION 2

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

A. Compliance is validated.

B. Boundaries are established.

C. Security automation is seamlessly integrated.

D. Access controls are enforced.

Correct Answer: BD

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. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Zero Trust Security Model], [Zero Trust Network Security]

QUESTION 3

What is a benefit of CN-Series firewalls securing traffic between pods and other workload types?

A. It protects data center and internet gateway deployments.

B. It allows for automatic deployment, provisioning, and immediate policy enforcement without any manual intervention.

C. It ensures consistent security across the entire environment.

D. It allows extension of Zero Trust Network Security to the most remote locations and smallest branches.

Correct Answer: B

Explanation: A benefit of CN-Series firewalls securing traffic between pods and other workload types is that it allows for automatic deployment, provisioning, and immediate policy enforcement without any manual intervention. CN-Series

firewalls are integrated with Kubernetes and use the Kubernetes API server to get information about pod labels, namespaces, services, and network policies. CN-Series firewalls can also use Panorama or Terraform to automate the

configuration and management of security policies.

References: [CN-Series Deployment Guide]

QUESTION 4

Which two statements apply to the VM-Series plugin? (Choose two.)

A. It can manage capabilities common to both VM-Series firewalls and hardware firewalls.

B. It can be upgraded independently of PAN-OS.

C. It enables management of cloud-specific interactions between VM-Series firewalls and supported public cloud platforms.

D. It can manage Panorama plugins.

Correct Answer: BC

Explanation: The two statements that apply to the VM-Series plugin are:

It can be upgraded independently of PAN-OS.

It enables management of cloud-specific interactions between VM-Series firewalls and supported public cloud platforms.

The VM-Series plugin is a software component that extends the functionality of the PAN- OS operating system to support cloud-specific features and APIs. The VM-Series plugin can be upgraded independently of PAN-OS to provide faster access to new cloud capabilities and integrations. The VM-Series plugin enables management of cloud-specific interactions between VM-Series firewalls and supported public cloud platforms, such as AWS, Azure, GCP, Alibaba Cloud, and

Oracle Cloud. These interactions include bootstrapping, licensing, scaling, high availability, load balancing, and tagging. The VM- Series plugin cannot manage capabilities common to both VM-Series firewalls and hardware firewalls, as those

are handled by PAN-OS. The VM-Series plugin cannot manage Panorama plugins, as those are separate software components that extend the functionality of the Panorama management server to support cloud-specific features and APIs.

References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [VM- Series Plugin Overview], [VM-Series Plugin Release Notes]

QUESTION 5

Which offering can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication?

A. OCSP

B. Secure Sockets Layer (SSL) Inbound Inspection

C. Advanced URL Filtering (AURLF)

D. WildFire

Correct Answer: B

Explanation: Secure Sockets Layer (SSL) Inbound Inspection is the offering that can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication. SSL Inbound Inspection is a feature that allows the firewall to decrypt and inspect inbound SSL/TLS traffic from external clients to internal servers. SSL Inbound Inspection can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication by applying threat prevention technologies, such as antivirus, anti-spyware, vulnerability protection, URL filtering, file blocking, data filtering, and WildFire analysis, to the decrypted traffic and blocking any malicious content or activity. OCSP, Advanced URL Filtering (AURLF), and WildFire are not offerings that can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication, but they are related solutions that can enhance security and visibility. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [SSL Inbound Inspection], [Threat Prevention Datasheet]