PCSFE^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.pass4itsure.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

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

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 2

Which protocol is used for communicating between VM-Series firewalls and a gateway load balancer in Amazon Web Services (AWS)?

A. VRLAN

B. Geneve

C. GRE

D. VMLAN

Correct Answer: B

Explanation: Geneve is the protocol used for communicating between VM-Series firewalls and a gateway load balancer in Amazon Web Services (AWS). A gateway load balancer is a type of network load balancer that distributes traffic across multiple virtual appliances, such as VM-Series firewalls, in AWS. Geneve is a tunneling protocol that encapsulates the original packet with an additional header that contains metadata about the source and destination endpoints, as well as other information. Geneve allows the gateway load balancer to preserve the original packet attributes and forward it to the appropriate VM- Series firewall for inspection and processing. VRLAN, GRE, and VMLAN are not protocols used for communicating between VM-Series firewalls and a gateway load balancer in AWS, but they are related concepts that can be used for other purposes. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploy the VM-Series Firewall with AWS Gateway Load Balancer], [Geneve Protocol Specification]

QUESTION 3

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 4

What does the number of required flex credits for a VM-Series firewall depend on?

A. vCPU allocation

B. IP address allocation

C. Network interface allocation

D. Memory allocation

Correct Answer: A

Explanation: The number of required flex credits for a VM-Series firewall depends on vCPU allocation. Flex 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 flex credits to provision VM-Series firewalls on any supported cloud or virtualization platform. The number of required flex credits for a VM-Series firewall depends on vCPU allocation, which is the number of virtual CPUs assigned to the VM-Series firewall instance. The vCPU allocation determines the performance and capacity of the VM-Series firewall instance, such as throughput, sessions, policies, rules, and features. The number of required flex credits for a VM-Series firewall does not depend on IP address allocation, network interface allocation, or memory allocation, as those are not factors that affect the licensing cost or consumption of flex credits. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Flex Credits Datasheet], [Flex Credits FAQ], [VM-Series System Requirements]

QUESTION 5

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

Correct 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. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Microsegmentation with Palo Alto Networks], [Microsegmentation for Dummies]

PCSFE PDF Dumps PCSFE Exam Questions PCSFE Braindumps