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

QUESTION 1

How is traffic directed to a Palo Alto Networks firewall integrated with Cisco ACI?

A. By using contracts between endpoint groups that send traffic to the firewall using a shared policy

B. Through a virtual machine (VM) monitor domain

C. Through a policy-based redirect

D. By creating an access policy

Correct Answer: C

Explanation: Traffic is directed to a Palo Alto Networks firewall integrated with Cisco ACI through a policy-based redirect. Cisco ACI is a software-defined network (SDN) solution that provides network automation, orchestration, and visibility. A policy-based redirect is a mechanism that allows Cisco ACI to redirect traffic from one endpoint group (EPG) to another EPG through a service device, such as a Palo Alto Networks firewall. The firewall can then inspect and enforce security policies on the redirected traffic before sending it back to Cisco ACI. Traffic is not directed to a Palo Alto Networks firewall integrated with Cisco ACI by using contracts between endpoint groups that send traffic to the firewall using a shared policy, through a virtual machine (VM) monitor domain, or by creating an access policy, as those are not valid methods for traffic redirection in Cisco ACI. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploy the VM-Series Firewall on Cisco ACI], [Cisco ACI Policy-Based Redirect]

QUESTION 2

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 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 the appropriate file format for Kubernetes applications?

A. .yaml

B. .exe

C. .json

D. .xml

Correct Answer: A

Explanation: The appropriate file format for Kubernetes applications is .yaml. YAML is a human-readable data serialization language that is commonly used for configuration files. Kubernetes applications are defined and deployed using YAML files that specify the desired state and configuration of the application components, such as pods, services, deployments, or ingresses. YAML files for Kubernetes applications follow a specific syntax and structure that adhere to the Kubernetes API specifications. .exe, .json, and .xml are not appropriate file formats for Kubernetes applications, but they are related formats that can be used for other purposes. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [What is YAML?], [Kubernetes Basics], [Kubernetes API Overview]

QUESTION 5

What can be implemented in a CN-Series to protect communications between Dockers?

A. Firewalling

B. Runtime security

C. Vulnerability management

D. Data loss prevention (DLP)

Correct Answer: A

Explanation: CN-Series firewall can protect communications between Dockers by firewalling. Dockers are software platforms that provide containerization technology for packaging and running applications in isolated environments. Communications between Dockers are network connections between containers within a Docker host or across Docker hosts. CN-Series firewall is a containerized firewall that integrates with Kubernetes and provides visibility and control over container traffic. CN-Series firewall can protect communications between Dockers by firewalling, which is the process of inspecting and enforcing security policies on network traffic based on application, user, content, and threat information. CN-Series firewall can also leverage threat prevention technologies, such as antivirus, anti-spyware, vulnerability protection, URL filtering, file blocking, data filtering, and WildFire analysis, to block any malicious content or activity in the communications between Dockers. CN-Series firewall does not protect communications between Dockers by runtime security, vulnerability management, or data loss prevention (DLP), as those are not features or functions of CN-Series firewall. References: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [CN-Series Datasheet], [CN-Series Concepts], [What is Docker?]