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.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What must be enabled when using Terraform templates with a Cloud next-generation firewall (NGFW) for Amazon Web Services (AWS)?

A. AWS CloudWatch logging

B. Access to the Cloud NGFW for AWS console

C. Access to the Palo Alto Networks Customer Support Portal

D. AWS Firewall Manager console access

Correct Answer: B

Explanation: Access to the Cloud NGFW for AWS console must be enabled when using Terraform templates with a Cloud next-generation firewall (NGFW) for Amazon Web Services (AWS). Terraform is an open-source tool that allows users to define and provision infrastructure as code using declarative configuration files. Terraform templates are files that specify the resources and configuration for deploying and managing infrastructure components, such as firewalls, load balancers, networks, or servers. Cloud NGFW for AWS is a cloud-native solution that provides comprehensive security and visibility across AWS environments, including VPCs, regions, accounts, and workloads. Cloud NGFW for AWS 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. Access to the Cloud NGFW for AWS console must be enabled when using Terraform templates with a Cloud NGFW for AWS, as the console is the web-based interface that allows customers to view and manage their Cloud NGFW for AWS instances, policies, logs, alerts, and reports. The console also provides the necessary information and credentials for integrating with Terraform, such as the API endpoint, access key ID, secret access key, and customer ID. AWS CloudWatch logging, access to the Palo Alto Networks Customer Support Portal, and AWS Firewall Manager console access do not need to be enabled when using Terraform templates with a Cloud NGFW for AWS, as those are not required or relevant components for Terraform integration. References: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [Terraform Overview], [Cloud Next-Generation Firewall Datasheet], [Cloud Next-Generation Firewall Deployment Guide], [Cloud Next- Generation Firewall Console Guide]

QUESTION 2

Which service, when enabled, provides inbound traffic protection?

A. Advanced URL Filtering (AURLF)

B. Threat Prevention

C. Data loss prevention (DLP)

D. DNS Security

Correct Answer: D

Explanation: DNS Security is a service that provides inbound traffic protection by preventing DNS-based attacks. DNS Security uses machine learning and threat intelligence to identify and block malicious domains, command and control (C2) traffic, and DNS tunneling. References: [DNS Security]

QUESTION 3

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 4

Which software firewall would help a prospect interested in securing an environment with Kubernetes?

A. KN-Series

B. ML-Series

C. VM-Series

D. CN-Series

Correct Answer: D

Explanation: CN-Series firewall is the software firewall that would help a prospect interested in securing an environment with Kubernetes. Kubernetes is a platform that provides orchestration, automation, and management of containerized applications. Kubernetes environment requires network security that can protect the inter-service communication from cyberattacks and enforce granular security policies based on application or workload characteristics. CN-Series firewall is a containerized firewall that integrates with Kubernetes and provides visibility and control over container traffic. CN-Series firewall can help a prospect interested in securing an environment with Kubernetes by inspecting and enforcing security policies on traffic between containers within a pod, across pods, or across namespaces in a Kubernetes cluster. KN-Series, ML-Series, VM- Series, and Cloud next-generation firewall are not software firewalls that would help a prospect interested in securing an environment with Kubernetes, but they are related solutions that can be deployed on different platforms or environments. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Datasheet], [CN- Series Concepts], [What is Kubernetes?]

QUESTION 5

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]