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

How are CN-Series firewalls licensed?

A. Data-plane vCPU

B. Service-plane vCPU

C. Management-plane vCPU

D. Control-plane vCPU

Correct Answer: A

Explanation: CN-Series firewalls are licensed by data-plane vCPU. Data-plane vCPU is the number of virtual CPUs assigned to the data plane of the CN-Series firewall instance. The data plane is the part of the CN-Series firewall that processes network traffic and applies security policies. CN-Series firewalls are licensed by data-plane vCPU, which determines the performance and capacity of the CN-Series firewall instance, such as throughput, sessions, policies, rules, and features. CN-Series firewalls are not licensed by service-plane vCPU, management-plane vCPU, or control-plane vCPU, as those are not factors that affect the licensing cost or consumption of CN-Series firewalls. References: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [CN-Series Licensing], [CN-Series System Requirements], [CN-Series Architecture]

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

What are two requirements for automating service deployment of a VM-Series firewall from an NSX Manager? (Choose two.)

A. vCenter has been given Palo Alto Networks subscription licenses for VM-Series firewalls.

B. Panorama has been configured to recognize both the NSX Manager and vCenter.

C. The deployed VM-Series firewall can establish communications with Panorama.

D. Panorama can establish communications to the public Palo Alto Networks update servers.

Correct Answer: BC

Explanation: The two requirements for automating service deployment of a VM-Series firewall from an NSX Manager are: Panorama has been configured to recognize both the NSX Manager and vCenter. The deployed VM-Series firewall can establish communications with Panorama. NSX Manager is a software component that provides centralized management and control of the NSX environment, including network virtualization, automation, and security. Service deployment is a process that involves deploying and configuring network services, such as firewalls, load balancers, or routers, on the NSX environment. VM-Series firewall is a virtualized version of the Palo Alto Networks next-generation firewall that can be deployed on various cloud or virtualization platforms, including NSX. Panorama is a centralized management server that provides visibility and control over multiple Palo Alto Networks firewalls and devices. Panorama has been configured to recognize both the NSX Manager and vCenter is a requirement for automating service deployment of a VM-Series firewall from an NSX Manager. vCenter is a software component that provides centralized management and control of the VMware environment, including hypervisors, virtual machines, and other resources. Panorama has been configured to recognize both the NSX Manager and vCenter by adding them as VMware service managers and enabling service insertion for VM-Series firewalls on NSX. This allows Panorama to communicate with the NSX Manager and vCenter, retrieve information about the NSX environment, and deploy and manage VM-Series firewalls as network services on the NSX environment. The deployed VM-Series firewall can establish communications with Panorama is a requirement for automating service deployment of a VM-Series firewall from an NSX Manager. The deployed VM-Series firewall can establish communications with Panorama by registering with Panorama using its serial number or IP address, and receiving configuration updates and policy rules from Panorama. This allows the VM-Series firewall to operate as part of the Panorama management domain, synchronize its settings and status with Panorama, and report its logs and statistics to Panorama. vCenter has been given Palo Alto Networks subscription licenses for VM-Series firewalls and Panorama can establish communications to the public Palo Alto Networks update servers are not requirements for automating service deployment of a VM-Series firewall from an NSX Manager, as those are not related or relevant factors for service deployment automation. References: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [Deploy the VM-Series Firewall on VMware NSX-T], [Panorama Overview], [VMware Service Manager], [Register the Firewall with Panorama]

QUESTION 4

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 5

Which two elements of the Palo Alto Networks platform architecture enable security orchestration in a software-defined network (SDN)? (Choose two.)

A. Full set of APIs enabling programmatic control of policy and configuration

B. VXLAN support for network-layer abstraction

C. Dynamic Address Groups to adapt Security policies dynamically

D. NVGRE support for advanced VLAN integration

Correct Answer: AC

Explanation: The two elements of the Palo Alto Networks platform architecture that enable security orchestration in a software-defined network (SDN) are: Full set of APIs enabling programmatic control of policy and configuration Dynamic Address Groups to adapt Security policies dynamically The Palo Alto Networks platform architecture consists of four key elements: natively integrated security technologies, full set of APIs, cloud-delivered services, and centralized management. The full set of APIs enables programmatic control of policy and configuration across the platform, allowing for automation and integration with SDN controllers and orchestration tools. Dynamic Address Groups are objects that represent groups of IP addresses based on criteria such as tags, regions, interfaces, or user-defined attributes. Dynamic Address Groups allow Security policies to adapt dynamically to changes in the network topology or workload characteristics without requiring manual updates. VXLAN support for network-layer abstraction and NVGRE support for advanced VLAN integration are not elements of the Palo Alto Networks platform architecture, but they are features that support SDN deployments. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Palo Alto Networks Platform Architecture], [API Overview], [Dynamic Address Groups Overview]

PCSFE PDF Dumps PCSFE Practice Test PCSFE Study Guide