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.certbus.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

Which two criteria are required to deploy VM-Series firewalls in high availability (HA)? (Choose two.)

A. Assignment of identical licenses and subscriptions

B. Deployment on a different host

C. Configuration of asymmetric routing

D. Deployment on same type of hypervisor

Correct Answer: AB

Explanation: To deploy VM-Series firewalls in high availability (HA), you need to assign identical licenses and subscriptions, and deploy them on a different host. Assigning identical licenses and subscriptions ensures that both firewalls have the same features and capabilities. Deploying them on a different host ensures that they are not affected by the same host failure. References: [VM-Series High Availability]

QUESTION 2

What Palo Alto Networks software firewall protects Amazon Web Services (AWS) deployments with network security delivered as a managed cloud service?

A. VM-Series

B. Cloud next-generation firewall

C. CN-Series

D. Ion-Series Ion-Series

Correct Answer: B

Explanation: Cloud next-generation firewall is the Palo Alto Networks software firewall that protects Amazon Web Services (AWS) deployments with network security delivered as a managed cloud service. Cloud next-generation firewall is a cloud-native solution that provides comprehensive security and visibility across AWS environments, including VPCs, regions, accounts, and workloads. Cloud next-generation firewall 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. VM-Series, CN-Series, and Ion-Series are not Palo Alto Networks software firewalls that protect AWS deployments with network security delivered as a managed cloud service, but they are related solutions that can be deployed on AWS or other platforms. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Cloud Next-Generation Firewall Datasheet], [VM-Series Datasheet], [CN-Series Datasheet], [Ion-Series Datasheet]

QUESTION 3

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 4

Which Palo Alto Networks firewall provides network security when deploying a microservices-based application?

A. PA-Series

B. ICN-Series

C. VM-Series

D. HA-Series

Correct Answer: B

Explanation: CN-Series firewall is the Palo Alto Networks firewall that provides network security when deploying a microservices-based application. A microservices-based application is an application that consists of multiple independent and loosely coupled services that communicate with each other through APIs. A microservices-based application 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 provide network security when deploying a microservices-based application by inspecting and enforcing security policies on traffic between containers within a pod, across pods, or across namespaces in a Kubernetes cluster. PA-Series, VM-Series, and HA-Series are not Palo Alto Networks firewalls that provide network security when deploying a microservices- based application, 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 a Microservices Architecture?]

QUESTION 5

What is a benefit of network runtime security?

A. It more narrowly focuses on one security area and requires careful customization integration and maintenance

B. It removes vulnerabilities that have been baked into containers.

C. It is siloed to enhance workload security.

D. It identifies unknown vulnerabilities that cannot be identified by known Common Vulnerability and Exposure (CVE) lists.

Correct Answer: D

Explanation: A benefit of network runtime security is that it identifies unknown vulnerabilities that cannot be identified by known Common Vulnerability and Exposure (CVE) lists. Network runtime security is a type of security that monitors and analyzes network traffic in real time to detect and prevent malicious activities or anomalous behaviors. Network runtime security can identify unknown vulnerabilities that cannot be identified by known CVE lists, such as zero-day exploits, advanced persistent threats, or custom malware. Network runtime security can also provide visibility and context into network activity, such as application dependencies, user identities, device types, or threat intelligence. Network runtime security does not more narrowly focus on one security area and requires careful customization, integration, and maintenance, remove vulnerabilities that have been baked into containers, or is siloed to enhance workload security, as those are not benefits or characteristics of network runtime security. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Network Runtime Security], [What is CVE?]

QUESTION 6

Which two features of CN-Series firewalls protect east-west traffic between pods in different trust zones? (Choose two.)

A. Intrusion prevention system

B. Communication with Panorama

C. External load balancer

D. Layer 7 visibility

Correct Answer: AD

Explanation: The two features of CN-Series firewalls that protect east-west traffic between pods in different trust zones are: Intrusion prevention system Layer 7 visibility East-west traffic is the traffic that flows between applications or workloads within a network or a cloud environment. Pods are the smallest units of deployment in Kubernetes, consisting of one or more containers that share resources and network space. Trust zones are segments of the network or the cloud environment that have different levels of security requirements or policies based on data sensitivity, user identity, device type, or application function. CN-Series firewalls are containerized firewalls that integrate with Kubernetes and provide visibility and control over container traffic. Intrusion prevention system is a feature of CN-Series firewalls that protects east-west traffic between pods in different trust zones by detecting and blocking known exploits and vulnerabilities using signature-based and behavior-based methods. Layer 7 visibility is a feature of CN-Series firewalls that protects east-west traffic between pods in different trust zones by identifying and classifying applications and protocols based on their content and characteristics, regardless of port, encryption, or evasion techniques. Communication with Panorama and external load balancer are not features of CN-Series firewalls that protect east-west traffic between pods in different trust zones, but they are related features that can enhance management and performance. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Concepts], [CN-Series Deployment Guide for Native K8], [Intrusion Prevention System Overview], [App-ID Overview]

QUESTION 7

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 8

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 9

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]

QUESTION 10

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 11

Which three NSX features can be pushed from Panorama in PAN-OS? (Choose three.)

A. Security group assignment of virtual machines (VMs)

B. Security groups

C. Steering rules

D. User IP mappings

E. Multiple authorization codes

Correct Answer: ABC

QUESTION 12

Which two configuration options does Palo Alto Networks recommend for outbound high availability (HA) design in Amazon Web Services using a VM-Series firewall? (Choose two.)

A. Transit VPC and Security VPC

B. Traditional active-active HA

C. Transit gateway and Security VPC

D. Traditional active-passive HA

Correct Answer: CD

Explanation: Palo Alto Networks recommends two configuration options for outbound high availability (HA) design in Amazon Web Services using a VM-Series firewall: transit gateway and Security VPC, and traditional active-passive HA. Transit gateway and Security VPC allows you to use a single transit gateway to route traffic between multiple VPCs and the internet, while using a Security VPC to host the VM-Series firewalls. Traditional active-passive HA allows you to use two VM-Series firewalls in an HA pair, where one firewall is active and handles all traffic, while the other firewall is passive and takes over in case of a failure. References: [VM-Series Deployment Guide for AWS Outbound VPC]

QUESTION 13

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 14

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?]

QUESTION 15

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]