PaloAltoNetworks.PCSFE.v2024-05-24.q23

Exam Code:	PCSFE
Exam Name:	Palo Alto Networks Certified Software Firewall Engineer
Certification Provider:	Palo Alto Networks
Free Question Number:	23
Version:	v2024-05-24
# of views:	1138
# of Questions views:	230
https://www.exam-tests.com/PCSFE-exam/PaloAltoNetworks.PCSFE.v2024-05-24.q23.html	

NEW QUESTION: 1
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
Answer: (SHOW ANSWER)
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. Reference: 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]

NEW QUESTION: 2
Which of the following can provide application-level security for a web-server instance on Amazon Web Services (AWS)?
A. VM-Series firewalls
B. Hardware firewalls
C. Terraform templates
D. Security groups
Answer: A (LEAVE A REPLY)
VM-Series firewalls can provide application-level security for a web-server instance on Amazon Web Services (AWS). VM-Series firewalls are virtualized versions of the Palo Alto Networks next-generation firewall that can be deployed on various cloud platforms, including AWS. VM-Series firewalls can protect web servers from cyberattacks by applying granular security policies based on application, user, content, and threat information. Hardware firewalls, Terraform templates, and security groups are not solutions that can provide application-level security for a web-server instance on AWS, but they are related concepts that can be used in conjunction with VM-Series firewalls. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [VM-Series on AWS], [VM-Series Datasheet], [Terraform for VM-Series on AWS], [Security Groups for Your VPC]

NEW QUESTION: 3
Why are VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster problematic for protecting containerized workloads?
A. They are located outside the cluster and have no visibility into application-level cluster traffic.
B. They do not scale independently of the Kubernetes cluster.
C. They are managed by another entity when located inside the cluster.
D. They function differently based on whether they are located inside or outside of the cluster.
Answer: (SHOW ANSWER)
VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster are problematic for protecting containerized workloads because they are located outside the cluster and have no visibility into application-level cluster traffic. Kubernetes is a platform that provides orchestration, automation, and management of containerized applications. Kubernetes cluster traffic consists of traffic between containers within a pod, across pods, or across namespaces. VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster cannot inspect or control this traffic, as they only see the encapsulated

or aggregated traffic at the network layer. This creates blind spots and security gaps for containerized workloads. VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster are not problematic for protecting containerized workloads because they do not scale independently of the Kubernetes cluster, are managed by another entity when located inside the cluster, or function differently based on whether they are located inside or outside of the cluster, as those are not valid reasons or scenarios for firewall deployment in a Kubernetes environment. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Concepts], [VM-Series on Kubernetes]

NEW QUESTION: 4
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.
Answer: B,C (LEAVE A REPLY)
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. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [VM-Series Plugin Overview], [VM-Series Plugin Release Notes]

NEW QUESTION: 5
Which component can provide application-based segmentation and prevent lateral threat movement?
A. DNS Security
B. NAT
C. URL Filtering

D. App-ID

Answer: D (LEAVE A REPLY)

App-ID is the component that can provide application-based segmentation and prevent lateral threat movement. Application-based segmentation is a method of dividing the network into smaller segments or zones based on application or workload characteristics, such as function, dependency, owner, or security posture. Lateral threat movement is a technique used by attackers to move across the network from one compromised host to another, looking for sensitive data or assets. App-ID is a feature that identifies and classifies applications and protocols based on their content and characteristics, regardless of port, encryption, or evasion techniques. App-ID can provide application-based segmentation and prevent lateral threat movement by applying granular security policies based on application information to each segment or connection, blocking unauthorized access or data exfiltration. DNS Security, NAT, and URL Filtering are not components that can provide application-based segmentation and prevent lateral threat movement, but they are related features that can enhance security and visibility. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [App-ID Overview], [Microsegmentation with Palo Alto Networks], [Lateral Movement]

NEW QUESTION: 6

Which offering inspects encrypted outbound traffic?

A. WildFire

B. TLS decryption

C. Content-ID

D. Advanced URL Filtering (AURLF)

Answer: B (LEAVE A REPLY)

TLS decryption is the offering that inspects encrypted outbound traffic. TLS decryption is a feature that allows the firewall to decrypt and inspect outbound SSL/TLS traffic from internal clients to external servers. TLS decryption can inspect encrypted outbound traffic by applying threat prevention technologies, such as antivirus, anti-spyware, vulnerability protection, URL filtering, file blocking, data filtering, and WildFire analysis, to the decrypted traffic and blocking any malicious content or activity. WildFire, Content-ID, and Advanced URL Filtering (AURLF) are not offerings that inspect encrypted outbound traffic, but they are related solutions that can enhance security and visibility. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [TLS Decryption Overview], [Threat Prevention Datasheet]

NEW QUESTION: 7

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)

Answer: (SHOW ANSWER)

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. Reference: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [CN-Series Datasheet], [CN-Series Concepts], [What is Docker?]

NEW QUESTION: 8

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

Answer: B (LEAVE A REPLY)

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. Reference: [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]

NEW QUESTION: 9
What is a design consideration for a prospect who wants to deploy VM-Series firewalls in an Amazon Web Services (AWS) environment?
A. Special AWS plugins are needed for load balancing.
B. Resources are shared within the cluster.
C. Only active-passive high availability (HA) is supported.
D. High availability (HA) clusters are limited to fewer than 8 virtual appliances.
Answer: C (LEAVE A REPLY)
A design consideration for a prospect who wants to deploy VM-Series firewalls in an Amazon Web Services (AWS) environment is that only active-passive high availability (HA) is supported. High availability (HA) is a feature that provides redundancy and failover protection for firewalls in case of hardware or software failure. Active-passive HA is a mode of HA that consists of two firewalls in a pair, where one firewall is active and handles all traffic, while the other firewall is passive and acts as a backup. Active-passive HA is the only mode of HA that is supported for VM-Series firewalls in an AWS environment, due to the limitations of AWS networking and routing. Active-active HA, which is another mode of HA that consists of two firewalls in a pair that both handle traffic and synchronize sessions, is not supported for VM-Series firewalls in an AWS environment. A design consideration for a prospect who wants to deploy VM-Series firewalls in an AWS environment is not that special AWS plugins are needed for load balancing, resources are shared within the cluster, or high availability (HA) clusters are limited to fewer than 8 virtual appliances, as those are not valid or relevant factors for firewall deployment in an AWS environment. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [High Availability Overview], [High Availability on AWS]

NEW QUESTION: 10
Which element protects and hides an internal network in an outbound flow?
A. DNS sinkholing
B. User-ID
C. App-ID
D. NAT
Answer: (SHOW ANSWER)

NAT is the element that protects and hides an internal network in an outbound flow. NAT is a feature that translates the source or destination IP address or port of a packet as it passes through the firewall. NAT can protect and hide an internal network in an outbound flow by replacing the private IP addresses of the internal hosts with a public IP address of the firewall or another device, making them appear as a single entity to the external network. This prevents external hosts from directly accessing or identifying the internal hosts, and also conserves the public IP address space. DNS sinkholing, User-ID, and App-ID are not elements that protect and hide an internal network in an outbound flow, but they are related features that can enhance security and visibility. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [NAT Overview], [DNS Sinkholing Overview], [User-ID Overview], [App-ID Overview]

NEW QUESTION: 11
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
Answer: A,C (LEAVE A REPLY)
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. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Licensing API Overview], [Licensing API Reference Guide]

NEW QUESTION: 12
Which two subscriptions should be recommended to a customer who is deploying VM-Series firewalls to a private data center but is concerned about protecting data-center resources from malware and lateral movement? (Choose two.)
A. Intelligent Traffic Offload
B. Threat Prevention
C. WildFire
D. SD-WAN
Answer: B,C (LEAVE A REPLY)
Threat Prevention and WildFire are the two subscriptions that provide protection against malware and lateral movement in a private data center. Threat Prevention blocks known threats using antivirus, anti-spyware, and vulnerability protection. WildFire analyzes unknown files and links in a cloud-based sandbox and generates signatures for new threats. Intelligent Traffic Offload is a feature that reduces the load on the firewall by offloading traffic that does not need inspection. SD-WAN is a feature that optimizes the performance and availability of WAN connections. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Threat Prevention Datasheet], [WildFire Datasheet], [Intelligent Traffic Offload], [SD-WAN]

NEW QUESTION: 13
Which two design options address split brain when configuring high availability (HA)? (Choose two.)
A. Adding a backup HA1 interface
B. Using the heartbeat backup
C. Bundling multiple interfaces in an aggregated interface group and assigning HA2
D. Sending heartbeats across the HA2 interfaces
Answer: A,B (LEAVE A REPLY)
The two design options that address split brain when configuring high availability (HA) are:
Adding a backup HA1 interface
Using the heartbeat backup
Split brain is a condition that occurs when both firewalls in an HA pair assume the active role and start processing traffic independently, resulting in traffic duplication, policy inconsistency, or session disruption. Split brain can be caused by network failures, device failures, or configuration errors that prevent the firewalls from communicating their HA status and synchronizing their configurations and sessions. Adding a backup HA1 interface is a design option that addresses split brain when configuring HA. The HA1 interface is used for exchanging HA state information and configuration synchronization between the firewalls. Adding a backup HA1 interface provides redundancy and failover protection for the HA1 interface, ensuring that the firewalls can maintain their HA communication and avoid split brain. Using the heartbeat backup is a design option that addresses split brain when configuring HA. The heartbeat backup is a mechanism that allows the firewalls to

send additional heartbeat messages through an alternate path, such as a management interface or a data interface, to verify the health of the peer firewall. Using the heartbeat backup prevents split brain caused by network failures or device failures that affect the primary HA interfaces. Bundling multiple interfaces in an aggregated interface group and assigning HA2, and sending heartbeats across the HA2 interfaces are not design options that address split brain when configuring HA, but they are related features that can enhance performance and reliability. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [High Availability Overview], [Configure HA Backup Links], [Configure Heartbeat Backup]

NEW QUESTION: 14
Regarding network segmentation, which two steps are involved in the configuration of a default route to an internet router? (Choose two.)
A. Select the Static Routes tab, then click Add.
B. Select Network > Interfaces.
C. Select the Config tab. then select New Route from the Security Zone Route drop-down menu.
D. Select Network > Virtual Router, then select the default link to open the Virtual Router dialog.
Answer: A,D (LEAVE A REPLY)
To configure a default route to an internet router, you need to select Network > Virtual Router, then select the default link to open the Virtual Router dialog. Then, select the Static Routes tab, then click Add. You can then specify the destination as 0.0.0.0/0 and the next hop as the IP address of the internet router1. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE)

NEW QUESTION: 15
How are CN-Series firewalls licensed?
A. Data-plane vCPU
B. Service-plane vCPU
C. Management-plane vCPU
D. Control-plane vCPU
Answer: A (LEAVE A REPLY)
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. Reference: [Palo Alto

Networks Certified Software Firewall Engineer (PCSFE)], [CN-Series Licensing], [CN-Series System Requirements], [CN-Series Architecture]

NEW QUESTION: 16
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
Answer: (SHOW ANSWER)
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.
Reference: [VM-Series Deployment Guide for AWS Outbound VPC]

NEW QUESTION: 17
How does a CN-Series firewall prevent exfiltration?
A. It employs custom-built signatures based on hash
B. It distributes incoming virtual private cloud (VPC) traffic across the pool of VM-Series firewalls.
C. It provides a license deactivation API key.
D. It inspects outbound traffic content and blocks suspicious activity.
Answer: (SHOW ANSWER)
CN-Series firewall prevents exfiltration by inspecting outbound traffic content and blocking suspicious activity. Exfiltration is a technique used by attackers to steal sensitive data or assets from a compromised network or system, usually by sending them to an external

destination, such as a command and control server, a drop zone, or an email address. CN-Series firewall is a containerized firewall that integrates with Kubernetes and provides visibility and control over container traffic. CN-Series firewall prevents exfiltration by inspecting outbound traffic content and blocking suspicious activity using threat prevention technologies, such as antivirus, anti-spyware, vulnerability protection, URL filtering, file blocking, data filtering, and WildFire analysis. CN-Series firewall does not prevent exfiltration by employing custom-built signatures based on hash, distributing incoming virtual private cloud (VPC) traffic across the pool of VM-Series firewalls, or providing a license deactivation API key, as those are not valid or relevant methods for exfiltration prevention. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Concepts], [CN-Series Deployment Guide for Native K8], [Threat Prevention Datasheet], [What is Exfiltration?]

NEW QUESTION: 18
Which two factors lead to improved return on investment for prospects interested in Palo Alto Networks virtualized next-generation firewalls (NGFWs)? (Choose two.)
A. Decreased likelihood of data breach
B. Reduced operational expenditures
C. Reduced time to deploy
D. Reduced insurance premiums
Answer: A,C (LEAVE A REPLY)
The two factors that lead to improved return on investment for prospects interested in Palo Alto Networks virtualized next-generation firewalls (NGFWs) are:
Decreased likelihood of data breach
Reduced time to deploy
Palo Alto Networks virtualized NGFWs are virtualized versions of the Palo Alto Networks next-generation firewall that can be deployed on various cloud or virtualization platforms. Palo Alto Networks virtualized NGFWs provide comprehensive security and visibility across hybrid and multi-cloud environments, protecting applications and data from cyberattacks. By using Palo Alto Networks virtualized NGFWs, prospects can decrease the likelihood of data breach by applying granular security policies based on application, user, content, and threat information, and by leveraging cloud-delivered services such as Threat Prevention, WildFire, URL Filtering, DNS Security, and Cortex Data Lake. By using Palo Alto Networks virtualized NGFWs, prospects can also reduce the time to deploy by taking advantage of automation and orchestration tools such as Terraform, Ansible, CloudFormation, ARM templates, and Panorama plugins that simplify and accelerate the deployment and configuration of firewalls across different cloud platforms. Reduced operational expenditures and reduced insurance premiums are not factors that lead to improved return on investment for prospects interested in Palo Alto Networks virtualized NGFWs, but they may be potential benefits or outcomes of using them. Reference: Palo

Alto Networks Certified Software Firewall Engineer (PCSFE), [VM-Series Datasheet], [CN-Series Datasheet], [Cloud Security Solutions]

NEW QUESTION: 19
Which component allows the flexibility to add network resources but does not require making changes to existing policies and rules?
A. Content-ID
B. External dynamic list
C. App-ID
D. Dynamic address group
Answer: D (LEAVE A REPLY)
Dynamic address group is the component that allows the flexibility to add network resources but does not require making changes to existing policies and rules. Dynamic address group is an object that represents a group of IP addresses based on criteria such as tags, regions, interfaces, or user-defined attributes. Dynamic address group allows Security policies to adapt dynamically to changes in the network topology or workload characteristics without requiring manual updates. Content-ID, External dynamic list, and App-ID are not components that allow the flexibility to add network resources but do not require making changes to existing policies and rules, but they are related features that can enhance security and visibility. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Dynamic Address Groups Overview], [Content-ID Overview], [External Dynamic Lists Overview], [App-ID Overview]

NEW QUESTION: 20
Why are containers uniquely suitable for runtime security based on allow lists?
A. Containers have only a few defined processes that should ever be executed.
B. Developers define the processes used in containers within the Dockerfile.
C. Docker has a built-in runtime analysis capability to aid in allow listing.
D. Operations teams know which processes are used within a container.
Answer: (SHOW ANSWER)
Containers are uniquely suitable for runtime security based on allow lists because containers have only a few defined processes that should ever be executed. Developers can specify the processes that are allowed to run in a container using a Dockerfile, but this does not guarantee that only those processes will run at runtime. Therefore, using an allow list approach can prevent any unauthorized or malicious processes from running in a container2. Reference: Container Security

NEW QUESTION: 21
When implementing active-active high availability (HA), which feature must be configured to allow the HA pair to share a single IP address that may be used as the network's gateway IP address?

A. VRRP
B. Floating IP address
C. ARP load sharing
D. HSRP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
With which two private cloud environments does Palo Alto Networks have deep integrations? (Choose two.)
A. VMware NSX-T
B. Cisco ACI
C. Dell APEX
D. Nutanix
Answer: A,B (LEAVE A REPLY)
The two private cloud environments that Palo Alto Networks have deep integrations with are:
VMware NSX-T
Cisco ACI
A private cloud environment is a cloud computing service that provides infrastructure as a service (IaaS) or platform as a service (PaaS) to customers within a private network or data center. A private cloud environment requires network security that can protect the traffic between different virtual machines (VMs) or other resources from cyberattacks and enforce granular security policies based on application, user, content, and threat information. Palo Alto Networks have deep integrations with VMware NSX-T and Cisco ACI, which are two private cloud environments that provide network virtualization, automation, and security for cloud-native applications. VMware NSX-T is a private cloud environment that provides software-defined networking (SDN) and security for heterogeneous endpoints and workloads across multiple hypervisors, containers, bare metal servers, or clouds. Cisco ACI is a private cloud environment that provides application-centric infrastructure (ACI) and security for physical and virtual endpoints across multiple data centers or clouds. Palo Alto Networks have deep integrations with VMware NSX-T and Cisco ACI by enabling features such as dynamic address groups, service insertion, policy redirection, service chaining, orchestration, monitoring, logging, and automation for VM-Series firewalls and Panorama on these platforms. Dell APEX and Nutanix are not private cloud environments that Palo Alto Networks have deep integrations with, but they are related platforms that can be used for other purposes. Reference: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [Deploy the VM-Series Firewall on VMware NSX-T], [Deploy the VM-Series Firewall on Cisco ACI], [What is VMware NSX-T?], [What is Cisco ACI?]

NEW QUESTION: 23

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

Answer: (SHOW ANSWER)

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. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Datasheet], [CN-Series Concepts], [What is a Microservices Architecture?]