Free Questions for PCSFE by actualtestdumps

Shared by Webb on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- Intrusion prevention system

B- Communication with Panorama

C- External load balancer

D- Layer 7 visibility

Answer:

A, D

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. 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]

Question 2

Question Type: **MultipleChoice**

Which offering inspects encrypted outbound traffic?

Options:

A- WildFire

B- TLS decryption

C- Content-ID

D- Advanced URL Filtering (AURLF)

Answer:

B

Explanation:

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]

Question 3

Question Type: MultipleChoice

What is the appropriate file format for Kubernetes applications?

Options:

A- .yaml

B- .exe

C- .json

D- .xml

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. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [What is YAML?], [Kubernetes Basics], [Kubernetes API Overview]

Question 4

Question Type: MultipleChoice

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

Options:

A- PA-Series

B- ICN-Series

C- VM-Series

D- HA-Series

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

Question 5

Question Type: MultipleChoice

Which offering can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication?

Options:

A- OCSP

B- Secure Sockets Layer (SSL) Inbound Inspection

C- Advanced URL Filtering (AURLF)

D- WildFire

Answer:

B

Explanation:

Secure Sockets Layer (SSL) Inbound Inspection is the offering that can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication. SSL Inbound Inspection is a feature that allows the firewall to decrypt and inspect inbound SSL/TLS traffic from external clients to internal servers. SSL Inbound Inspection can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication 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. OCSP, Advanced URL Filtering (AURLF), and WildFire are not offerings that can gain visibility and prevent an attack by a malicious actor attempting to exploit a known web server vulnerability using encrypted communication, but they are related solutions that can enhance security and visibility. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [SSL Inbound Inspection], [Threat Prevention Datasheet]

Question 6

Question Type: MultipleChoice

Where do CN-Series devices obtain a VM-Series authorization key?

Options:

A- Panorama

B- Local installation

C- GitHub

D- Customer Support Portal

Answer:

A

Explanation:

CN-Series devices obtain a VM-Series authorization key from Panorama. Panorama is a centralized management server that provides visibility and control over multiple Palo Alto Networks firewalls and devices. A VM-Series authorization key is a license key that activates the VM-Series firewall features and capacities. CN-Series devices obtain a VM-Series authorization key from Panorama by registering with Panorama using their CPU ID and requesting an authorization code from Panorama's license pool. Panorama then generates an authorization key for the CN-Series device and sends it back to the device for activation. CN-Series devices do not obtain a VM-Series authorization key from local installation, GitHub, or Customer Support Portal, as those are not valid or relevant sources for license management. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Panorama Overview], [VM-Series Licensing Overview], [CN-Series Licensing]

Question 7

Question Type: MultipleChoice

Which two design options address split brain when configuring high availability (HA)? (Choose two.)

Options:

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

Explanation:

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]

Question 8

Question Type: MultipleChoice

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?

Options:

A- ARP load sharing

B- Floating IP address

C- HSRP

D- VRRP

Answer:

B

Question 9

Question Type: MultipleChoice

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

Options:

A- Security group assignment of virtual machines (VMs)

B- Security groups

C- Steering rules

D- User IP mappings

E- Multiple authorization codes

Answer:

A, B, C

Question 10

Question Type: MultipleChoice

What is a design consideration for a prospect who wants to deploy VM-Series firewalls in an Amazon Web Services (AWS) environment?

Options:

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

Explanation:

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]

Question 11

Question Type: MultipleChoice

What is a benefit of network runtime security?

Options:

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.

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. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Network Runtime Security], [What is CVE?]