Free Questions for PCSFE by certscare

Shared by Fletcher on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which of the following can provide application-level security for a web-server instance on Amazon Web Services (AWS)?

Options:

A- VM-Series firewalls

B- Hardware firewalls

C- Terraform templates

D- Security groups

Answer:

A

Explanation:

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]

Question 2

Question Type: MultipleChoice

Which feature provides real-time analysis using machine learning (ML) to defend against new and unknown threats?

Options:

A- Advanced URL Filtering (AURLF)

B- Cortex Data Lake

C- DNS Security

D- Panorama VM-Series plugin

Answer:

C

Explanation:

DNS Security is the feature that provides real-time analysis using machine learning (ML) to defend against new and unknown threats. DNS Security leverages a cloud-based service that applies predictive analytics, advanced ML, and automation to block malicious domains and stop attacks in progress. Advanced URL Filtering (AURLF), Cortex Data Lake, and Panorama VM-Series plugin are not features that provide real-time analysis using ML, but they are related solutions that can enhance security and visibility. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [DNS Security Datasheet], [Advanced URL Filtering Datasheet], [Cortex Data Lake Datasheet], [Panorama VM-Series Plugin]

Question 3

Question Type: MultipleChoice

A CN-Series firewall can secure traffic between which elements?

Options:

A- Host containers

B- Source applications

C- Containers

D- IPods

Answer:

C

Explanation:

Containers are the elements that a CN-Series firewall can secure traffic between. Containers are isolated units of software that run on a shared operating system and have their own resources, dependencies, and configuration. A CN-Series firewall can inspect and enforce security policies on traffic between containers within a pod, across pods, or across namespaces in a Kubernetes cluster. Host containers, source applications, and IPods are not valid elements that a CN-Series firewall can secure traffic between. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Concepts], [What is a Container?]

Question 4

Question Type: MultipleChoice

Which solution is best for securing an EKS environment?

Options:

A- VM-Series single host

B- CN-Series high availability (HA) pair

C- PA-Series using load sharing

D- API orchestration

Answer:

B

Explanation:

CN-Series high availability (HA) pair is the best solution for securing an EKS environment. EKS is a managed service that allows users to run Kubernetes clusters on AWS. CN-Series is a containerized firewall that integrates with Kubernetes and provides visibility and control over container traffic. CN-Series HA pair consists of two CN-Series firewalls deployed in active-passive mode to provide redundancy and failover protection. VM-Series single host, PA-Series using load sharing, and API orchestration are not optimal solutions for securing an EKS environment, as they do not offer the same level of integration, scalability, and automation as CN-Series.

Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Deployment Guide for AWS EKS], [CN-Series Datasheet]

Question 5

Question Type: **MultipleChoice**

Which technology allows for granular control of east-west traffic in a software-defined network?

Options:

A- Routing

B- Microseqmentation

C- MAC Access Control List

D- Virtualization

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. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Microsegmentation with Palo Alto Networks], [Microsegmentation for Dummies]

Question 6

Question Type: MultipleChoice

Which two mechanisms could trigger a high availability (HA) failover event? (Choose two.)

Options:

A- Heartbeat polling

B- Ping monitoring

C- Session polling

D- Link monitoring

Answer:

A, D

Explanation:

Heartbeat polling and link monitoring are two mechanisms that can trigger an HA failover event. Heartbeat polling is a method of verifying the health of the peer firewall by sending periodic heartbeat messages. If the heartbeat messages are not received within a specified interval, the firewall assumes that the peer is down and initiates a failover. Link monitoring is a method of verifying the connectivity of the interfaces on the firewall by sending link state packets. If the link state packets are not received on a specified number of interfaces, the firewall assumes that the network is down and initiates a failover. Ping monitoring and session polling are not HA mechanisms, but they are used for path monitoring and session synchronization respectively. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [High Availability Overview], [Configure HA Link Monitoring], [Configure HA Path Monitoring], [Configure Session Synchronization]

Question 7

Question Type: **MultipleChoice**

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.)

Options:

A- Intelligent Traffic Offload

B- Threat Prevention

C- WildFire

D- SD-WAN

Answer:

B, C

Explanation:

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]

Question 8

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 9

Question Type: MultipleChoice

Which two actions can be performed for VM-Series firewall licensing by an orchestration system? (Choose two.)

Options:

A- Creating a license

B- Renewing a license

C- Registering an authorization code

D- Downloading a content update

Answer:

A, C

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. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Licensing API Overview], [Licensing API Reference Guide]

Question 10

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 11

Question Type: **MultipleChoice**

Which two routing options are supported by VM-Series? (Choose two.)

Options:

A- OSPF

B- RIP

C- BGP

D- IGRP

Answer:

A, C

Explanation:

The two routing options that are supported by VM-Series are:

OSPF

BGP

Routing is a process that determines the best path for sending network packets from a source to a destination. Routing options are protocols or methods that enable routing between different networks or devices. 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. VM-Series firewall supports various routing options that allow it to participate in dynamic routing environments and exchange routing information with other routers or devices. OSPF and BGP are two routing options that are supported by VM-Series. OSPF is a routing option that uses link-state routing algorithm to determine the shortest path between routers within an autonomous system (AS). BGP is a routing option that uses path vector routing algorithm to determine the best path between routers across different autonomous systems (ASes). RIP and IGRP are not routing options that are supported by VM-Series, but they are related protocols that can be used for other purposes. Reference: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [VM-Series Deployment Guide], [Routing Overview], [What is OSPF?], [What is BGP?]

Question 12

Question Type: MultipleChoice

Which two mechanisms could trigger a high availability (HA) failover event? (Choose two.)

Options:

A- Heartbeat polling

B- Ping monitoring

C- Session polling

D- Link monitoring

Answer:

A, D

Explanation:

Heartbeat polling and link monitoring are two mechanisms that can trigger an HA failover event. Heartbeat polling is a method of verifying the health of the peer firewall by sending periodic heartbeat messages. If the heartbeat messages are not received within a specified interval, the firewall assumes that the peer is down and initiates a failover. Link monitoring is a method of verifying the connectivity of the interfaces on the firewall by sending link state packets. If the link state packets are not received on a specified number of interfaces, the firewall assumes that the network is down and initiates a failover. Ping monitoring and session polling are not HA mechanisms, but they are used for path monitoring and session synchronization respectively. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [High Availability Overview], [Configure HA Link Monitoring], [Configure HA Path Monitoring], [Configure Session Synchronization]