PCSFE$^{Q\&As}$

Palo Alto Networks Certified Software Firewall Engineer (PCSFE)

Pass Palo Alto Networks PCSFE Exam with 100% Guarantee

QUESTION 1

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

A. Heartbeat polling

B. Ping monitoring

C. Session polling

D. Link monitoring

Correct Answer: AD

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. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [High Availability Overview], [Configure HA Link Monitoring], [Configure HA Path Monitoring], [Configure Session Synchronization]

QUESTION 2

What is the structure of the YAML Ain\\'t Markup Language (YAML) file repository?

A. Deployment Type/Kubernetes/Environment

B. Kubernetes/Deployment Type/Environment

C. Kubernetes/Environment/Deplovment Type

D. Environment/Kubernetes/Deployment Type

Correct Answer: B

Explanation: Kubernetes/Deployment Type/Environment is the structure of the YAML Ain\\'t Markup Language (YAML) file repository. YAML is a human-readable data serialization language that is commonly used for configuration files. YAML file repository is a collection of YAML files that specify the resources and configuration for deploying and managing infrastructure components, such as firewalls, load balancers, networks, or servers. Kubernetes/Deployment Type/Environment is the structure of the YAML file repository that organizes the YAML files based on the following criteria: Kubernetes: The platform that provides orchestration, automation, and management of containerized applications. Deployment Type: The method or model of deploying and managing infrastructure components, such as Terraform, Ansible, Helm, or Kubernetes manifests. Environment: The type or stage of the cloud or virtualization environment, such as development, testing, staging, or production. Deployment Type/Kubernetes/Environment, Kubernetes/Environment/Deployment Type, and Environment/Kubernetes/Deployment Type are not the structure of the YAML file repository, but they are related ways of organizing YAML files based on different criteria. References: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [What is YAML?], [YAML File Repository]

QUESTION 3

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

A. Host containers

B. Source applications

C. Containers

D. IPods

Correct 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. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Concepts], [What is a Container?]

QUESTION 4

Auto scaling templates for which type of firewall enable deployment of a single auto scaling group (ASG) of VM-Series firewalls to secure inbound traffic from the internet to Amazon Web Services (AWS) application workloads?

A. HA-Series

B. CN-Series

C. IPA-Series

D. VM-Series

Correct Answer: D

Explanation: Auto scaling templates for VM-Series firewalls enable deployment of a single auto scaling group (ASG) of VM-Series firewalls to secure inbound traffic from the internet to Amazon Web Services (AWS) application workloads. An ASG is a collection of EC2 instances that share similar characteristics and can be scaled up or down automatically based on demand or predefined conditions. Auto scaling templates for VM-Series firewalls are preconfigured templates that provide the necessary resources and configuration to deploy and manage VM-Series firewalls in an ASG on AWS. Auto scaling templates for VM-Series firewalls can be used to secure inbound traffic from the internet to AWS application workloads by placing the ASG of VM-Series firewalls behind an AWS Application Load Balancer (ALB) or a Gateway Load Balancer (GWLB) that distributes the traffic across the firewalls. The firewalls can then inspect and enforce security policies on the inbound traffic before sending it to the application workloads. Auto scaling templates for HA-Series, CN-Series, and IPA-Series firewalls do not enable deployment of a single ASG of VM-Series firewalls to secure inbound traffic from the internet to AWS application workloads, as those are different types of firewalls that have different deployment models and use cases. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Auto Scaling the VM-Series Firewall on AWS], [VM-Series Datasheet], [HA- Series Datasheet], [CN-Series Datasheet], [IPA-Series Datasheet]

QUESTION 5

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 6

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

A. OCSP

B. Secure Sockets Layer (SSL) Inbound Inspection

C. Advanced URL Filtering (AURLF)

D. WildFire

Correct 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. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [SSL Inbound Inspection], [Threat Prevention Datasheet]

QUESTION 7

How must a Palo Alto Networks Next-Generation Firewall (NGFW) be configured in order to secure traffic in a Cisco ACI environment?

A. It must be deployed as a member of a device cluster

B. It must use a Layer 3 underlay network

C. It must receive all forwarding lookups from the network controller

D. It must be identified as a default gateway

Correct Answer: B

Explanation: A Palo Alto Networks Next-Generation Firewall (NGFW) must be configured to use a Layer 3 underlay network in order to secure traffic in a Cisco ACI environment. A Layer 3 underlay network is a physical network that provides IP connectivity between devices, such as routers, switches, and firewalls. A Palo Alto Networks NGFW must use a Layer 3 underlay network to communicate with the Cisco ACI fabric and receive traffic redirection from the Cisco ACI policy-based redirect mechanism. A Palo Alto Networks NGFW does not need to be deployed as a member of a device cluster, receive all forwarding lookups from the network controller, or be identified as a default gateway in order to secure traffic in a Cisco ACI environment, as those are not valid requirements or options for firewall integration with Cisco ACI. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploy the VM-Series Firewall on Cisco ACI], [Cisco ACI Underlay Network]

QUESTION 8

How are Palo Alto Networks Next-Generation Firewalls (NGFWs) deployed within a Cisco ACI architecture?

A. SDN code hooks can help detonate malicious file samples designed to detect virtual environments.

B. Traffic can be automatically redirected using static address objects.

C. Service graphs are configured to allow their deployment.

D. VXLAN or NVGRE traffic is terminated and inspected for translation to VLANs.

Correct Answer: C

Explanation: Palo Alto Networks Next-Generation Firewalls (NGFWs) are deployed within a Cisco ACI architecture using service graphs. Service graphs are logical representations of how traffic flows through different network services, such as firewalls, load balancers, or routers. By configuring service graphs, you can insert NGFWs into the traffic path and apply security policies to the traffic. References: [Palo Alto Networks NGFW Integration with Cisco ACI]

QUESTION 9

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

A. Panorama

B. Local installation

C. GitHub

D. Customer Support Portal

Correct 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. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Panorama Overview], [VM-Series Licensing Overview], [CN-Series Licensing]

QUESTION 10

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.

Correct Answer: AD

Explanation: 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. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE)

QUESTION 11

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]

QUESTION 12

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

Correct 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. References: 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 13

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 14

Which two methods of Zero Trust implementation can benefit an organization? (Choose two.)

A. Compliance is validated.

B. Boundaries are established.

C. Security automation is seamlessly integrated.

D. Access controls are enforced.

Correct Answer: BD

Explanation: The two methods of Zero Trust implementation that can benefit an organization are: Boundaries are established Access controls are enforced Zero Trust is a security model that assumes no trust for any entity or network segment, and requires continuous verification and validation of all connections and transactions. Zero Trust implementation can benefit an organization by improving its security posture, reducing its attack surface, and enhancing its visibility and compliance. Boundaries are established is a method of Zero Trust implementation that involves defining and segmenting the network into smaller zones based on data sensitivity, user identity, device type, or application function. Boundaries are established can benefit an organization by isolating and protecting critical assets from unauthorized access or lateral movement. Access controls are enforced is a method of Zero Trust implementation that involves applying granular security policies based on the principle of least privilege to each zone or connection. Access controls are enforced can benefit an organization by preventing data exfiltration, malware propagation, or credential theft. Compliance is validated and security automation is seamlessly integrated are not methods of Zero Trust implementation, but they may be potential outcomes or benefits of implementing Zero Trust. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Zero Trust Security Model], [Zero Trust Network Security]

QUESTION 15

What are two environments supported by the CN-Series firewall? (Choose two.)

A. Positive K

B. OpenShift

C. OpenStack

D. Native K8

Correct Answer: BD

Explanation: The two environments supported by the CN-Series firewall are: OpenShift Native K8 The CN-Series firewall is a containerized firewall that integrates with Kubernetes and provides visibility and control over container traffic. The CN-Series firewall can be deployed in various environments that support Kubernetes, such as public clouds, private clouds, or on-premises data centers. OpenShift is an environment supported by the CN-Series firewall. OpenShift is a platform that provides enterprise-grade Kubernetes and container orchestration, as well as developer tools and services. Native K8 is an environment supported by the CN-Series firewall. Native K8 is a term that refers to the standard Kubernetes distribution that is available from the Kubernetes project website, without any vendor-specific modifications or additions. Positive K and OpenStack are not environments supported by the CN-Series firewall, but they are related concepts that can be used for other purposes. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Datasheet], [CN-Series Deployment Guide for OpenShift], [CN- Series Deployment Guide for Native K8], [What is OpenShift?], [What is Kubernetes?]

Latest PCSFE Dumps PCSFE Study Guide PCSFE Braindumps