Vendor: Palo Alto Networks

Exam Code: PCSFE

Exam Name: Palo Alto Networks Certified Software Firewall Engineer

Version: DEMO

QUESTION 1
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

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.

QUESTION 2
Which component scans for threats in allowed traffic?

A. Intelligent Traffic Offload
B. TLS decryption
C. Security profiles
D. NAT

Answer: C
Explanation:
Security profiles are the components that scan for threats in allowed traffic. Security profiles are sets of rules or settings that define how the firewall will inspect and handle traffic based on various threat prevention technologies, such as antivirus, anti-spyware, vulnerability protection, URL filtering, file blocking, data filtering, and WildFire analysis. Security profiles can be applied to Security policy rules to enforce granular protection against known and unknown threats in allowed traffic. Intelligent Traffic Offload, TLS decryption, and NAT are not components that scan for threats in allowed traffic, but they are related features that can enhance security and performance.

QUESTION 3
Which two deployment modes of VM-Series firewalls are supported across NSX-T? (Choose two.)

A. Prism Central

B. Bootstrap
C. Service Cluster
D. Host-based

Answer: CD
Explanation:
https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/set-up-the-vm-series-firewall-on-nsx/set-up-the-vm-series-firewall-on-nsx-t-east-west/supported-deployments-of-the-vm-series-firewall-on-vmware-nsx-t-ew

QUESTION 4
A customer in a VMware ESXi environment wants to add a VM-Series firewall and partition an existing group of virtual machines (VMs) in the same subnet into two groups. One group requires no additional security, but the second group requires substantially more security.
How can this partition be accomplished without editing the IP addresses or the default gateways of any of the guest VMs?

A. Edit the IP address of all of the affected VMs.
B. Create a new virtual switch and use the VM-Series firewall to separate virtual switches using virtual wire mode. Then move the guests that require more security into the new virtual switch.
C. Create a Layer 3 interface in the same subnet as the VMs and then configure proxy Address Resolution Protocol (ARP).
D. Send the VLAN out of the virtual environment into a hardware Palo Alto Networks firewall in Layer 3 mode. Use the same IP address as the old default gateway, then delete it.

Answer: B
Explanation:
The partition can be accomplished without editing the IP addresses or the default gateways of any of the guest VMs by creating a new virtual switch and using the VM-Series firewall to separate virtual switches using virtual wire mode. Then move the guests that require more security into the new virtual switch. A virtual switch is a software-based switch that connects virtual machines (VMs) in a VMware ESXi environment. A virtual wire is a deployment mode of the VM-Series firewall that allows it to act as a bump in the wire between two network segments, without requiring an IP address or routing configuration. By creating a new virtual switch and using the VM-Series firewall to separate virtual switches using virtual wire mode, the customer can isolate the group of VMs that require more security from the rest of the network, and apply security policies to the traffic passing through the firewall. The partition cannot be accomplished without editing the IP addresses or the default gateways of any of the guest VMs by editing the IP address of all of the affected VMs, creating a Layer 3 interface in the same subnet as the VMs and then configuring proxy Address Resolution Protocol (ARP), or sending the VLAN out of the virtual environment into a hardware Palo Alto Networks firewall in Layer 3 mode. Use the same IP address as the old default gateway, then delete it, as those methods would require changing the network configuration of the guest VMs or introducing additional complexity and latency.

QUESTION 5
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.

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.

QUESTION 6
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 (EDL)
C. App-ID
D. Dynamic address group

Answer: D
Explanation:
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.

QUESTION 7
Which PAN-OS feature allows for automated updates to address objects when VM-Series firewalls are setup as part of an NSX deployment?

A. Boundary automation
B. Hypervisor integration
C. Bootstrapping
D. Dynamic Address Group

Answer: D
Explanation:
Dynamic Address Group is the PAN-OS feature that allows for automated updates to address objects when VM-Series firewalls are setup as part of an NSX deployment. NSX is a software-defined network (SDN) solution that provides network virtualization, automation, and security for cloud-native applications. 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. When VM-Series firewalls are setup as part of an NSX deployment, they can leverage the NSX tags assigned to virtual machines (VMs) or containers by the NSX manager or controller to populate Dynamic Address

Groups and update Security policies accordingly. Boundary automation, Hypervisor integration, and Bootstrapping are not PAN-OS features that allow for automated updates to address objects when VM-Series firewalls are setup as part of an NSX deployment, but they are related concepts that can be used for other purposes.

QUESTION 8
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: AC
Explanation:
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.

QUESTION 9
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. PA-Series
D. VM-Series

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.

QUESTION 10
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 (NGFW)
C. CN-Series
D. Ion-Series Ion-Series

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.

QUESTION 11
What do tags allow a VM-Series firewall to do in a virtual environment?

A. Enable machine learning (ML).
B. Adapt Security policy rules dynamically.
C. Integrate with security information and event management (SIEM) solutions.
D. Provide adaptive reporting.

Answer: B
Explanation:
Tags allow a VM-Series firewall to adapt Security policy rules dynamically in a virtual environment. Tags are labels or identifiers that can be assigned to virtual machines (VMs), containers, or other resources in a virtual environment. Tags can be used to group resources based on various criteria, such as application, function, location, owner, or security posture. A VM-Series firewall can leverage tags to populate Dynamic Address Groups and update Security policies accordingly, without requiring manual changes. Tags do not enable machine learning (ML), integrate with security information and event management (SIEM) solutions, or provide adaptive reporting, but they are related features that can enhance security and visibility.

QUESTION 12
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.

Answer: BD
Explanation:
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.

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

Answer: AC
Explanation:
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.

QUESTION 14
What are two environments supported by the CN-Series firewall? (Choose two.)

A. Positive K
B. OpenShift
C. OpenStack
D. Native K8

Answer: BD
Explanation:
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.

QUESTION 15
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: A
Explanation:
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.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**