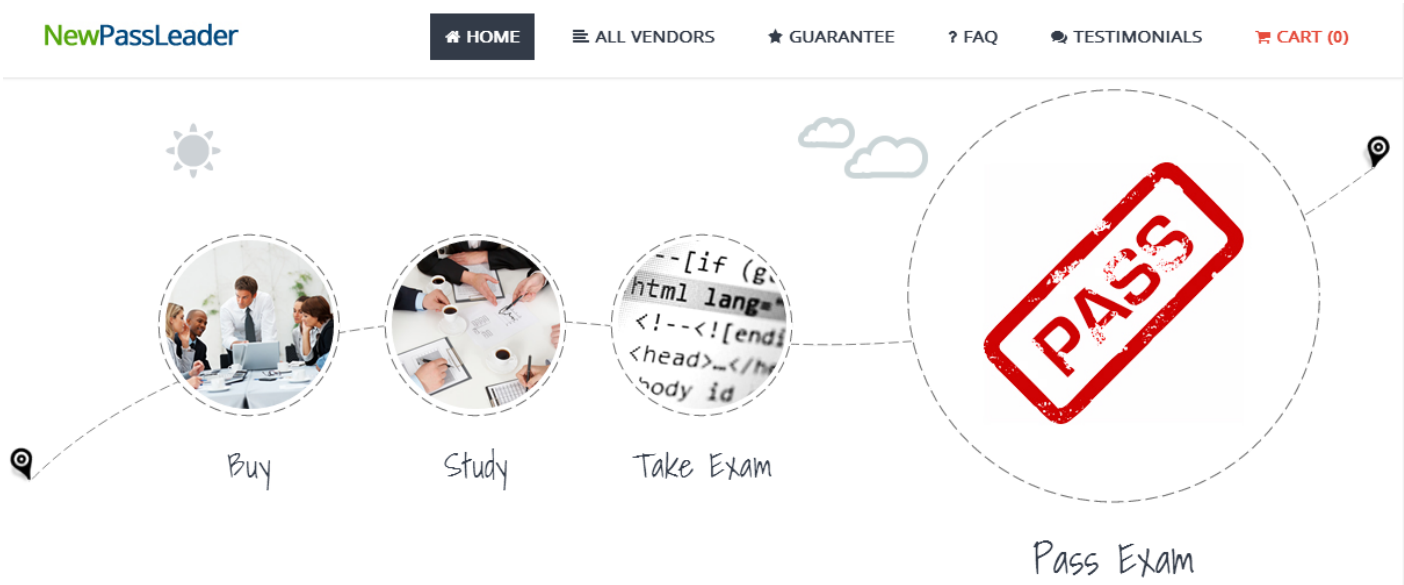
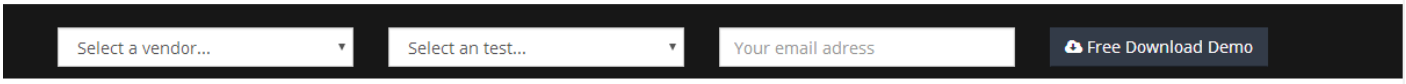
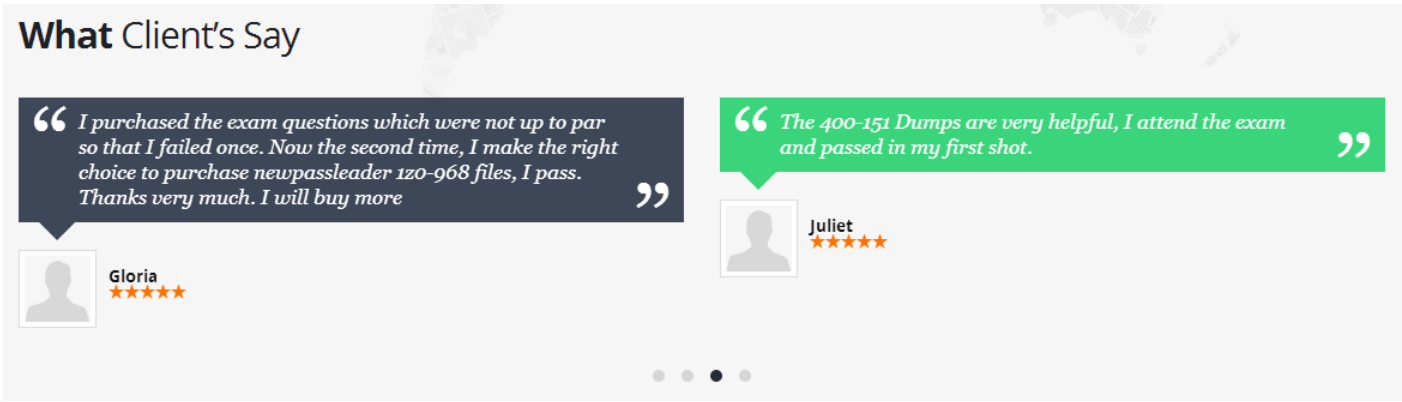
NewPassleader





Try **PDF Demo** before you buy

Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.
PDF format: Easy to read and print learning materials, our products are available in PDF file format.
Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.



http://www.newpassleader.com/

Attentive Service Exam Torrent and Valid Dumps - NewPassLeader

Exam : **PCSFE**

Title : Palo Alto Networks Certified Software Firewall Engineer

Vendor : Palo Alto Networks

Version : DEMO

NO.1 Which solution is best for securing an EKS environment?

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]

NO.2 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: C,D

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. Reference: [VM-Series Deployment Guide for AWS Outbound VPC]

NO.3 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: D

Explanation:

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?]

NO.4 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. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploy the VM-Series Firewall on Cisco ACI], [Cisco ACI Underlay Network]

NO.5 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: A

Explanation:

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

NO.6 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. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Tagging Overview], [Dynamic Address Groups Overview]

NO.7 Which protocol is used for communicating between VM-Series firewalls and a gateway load balancer in Amazon Web Services (AWS)?
A. VRLAN
B. Geneve
C. GRE
D. VMLAN
Answer: B
Explanation:
Geneve is the protocol used for communicating between VM-Series firewalls and a gateway load balancer in Amazon Web Services (AWS). A gateway load balancer is a type of network load balancer that distributes traffic across multiple virtual appliances, such as VM-Series firewalls, in AWS. Geneve is a tunneling protocol that encapsulates the original packet with an additional header that contains metadata about the source and destination endpoints, as well as other information. Geneve allows the gateway load balancer to preserve the original packet attributes and forward it to the appropriate VM-Series firewall for inspection and processing. VRLAN, GRE, and VMLAN are not protocols used for communicating between VM-Series firewalls and a gateway load balancer in AWS, but they are related concepts that can be used for other purposes. Reference: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploy the VM-Series Firewall with AWS Gateway Load Balancer], [Geneve Protocol Specification]