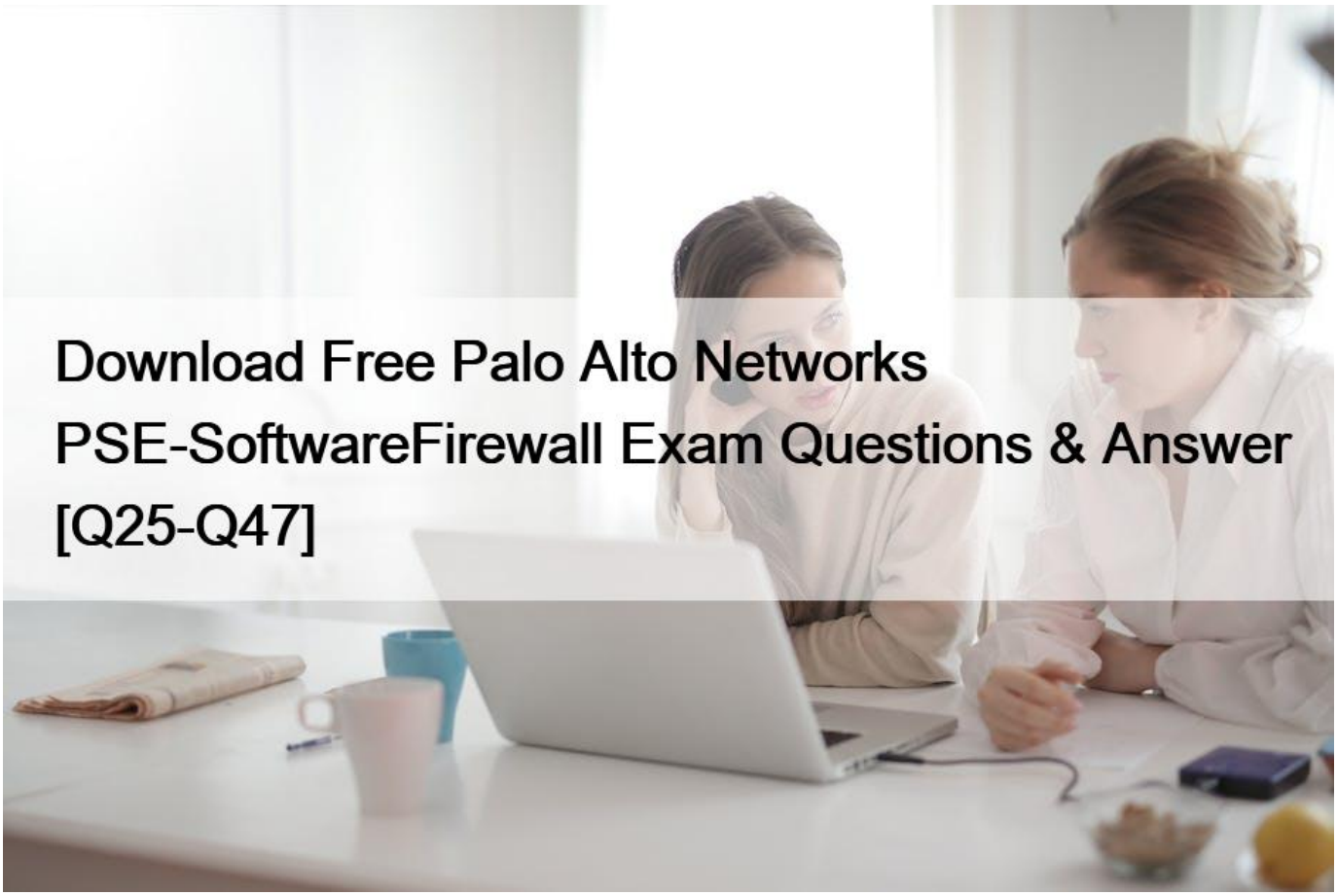
Download Free Palo Alto Networks PSE-SoftwareFirewall Exam Questions & Answer [Q25-Q47



Download Free Palo Alto Networks PSE-SoftwareFirewall Exam Questions & Answer
Online VALID PSE-SoftwareFirewall Exam Dumps File Instantly

Q25. How does Prisma Cloud Compute offer workload security at runtime?
* It quarantines containers that demonstrate increased CPU and memory usage.
* It automatically patches vulnerabilities and compliance issues for every container and service.
* It works with the identity provider (IdP) to identify overprivileged containers and services, and it restricts network access.
* It automatically builds an allow-list security model for every container and service.

Allow-list Security Model:

* Prisma Cloud Compute provides runtime security by automatically creating an allow-list security model for each container and service. This model ensures that only expected and authorized behaviors are allowed, effectively preventing unauthorized activities.

Q26. Which two factors lead to improved return on investment for prospects interested in Palo Alto Networks virtualized next-generation firewalls (NGFWs)? (Choose two.)
* Reduced operational expenditures
* Decreased likelihood of data breach

* Reduced insurance premiums
* Reduced time to deploy

Prospects interested in Palo Alto Networks virtualized next-generation firewalls (NGFWs) can achieve improved return on investment (ROI) through the following factors:

* Reduced operational expenditures: Virtualized NGFWs reduce the need for physical hardware, lowering the costs associated with purchasing, maintaining, and managing hardware appliances. This also includes savings on power, cooling, and physical space requirements.

Q27. 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?

* Edit the IP address of all of the affected VMs.
* 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.
* 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.
* Create a Layer 3 interface in the same subnet as the VMs and then configure proxy Address Resolution Protocol (ARP).

Creating a New Virtual Switch:

* By creating a new virtual switch, you can segment the network within the ESXi environment. The VM-Series firewall can then be used to provide security controls between these virtual switches using virtual wire mode.

Q28. Which PAN-OS feature allows for automated updates to address objects when VM-Series firewalls are setup as part of an NSX deployment?

* Dynamic Address Group
* Hypervisor integration
* Bootstrapping
* Boundary automation

Dynamic Address Groups in PAN-OS allow for automated updates to address objects when VM-Series firewalls are set up as part of an NSX deployment. These address groups can dynamically include members based on criteria such as tags, enabling automated and flexible security policies that adjust to changes in the virtual environment.

References:

* Palo Alto Networks Dynamic Address Groups: Dynamic Address Groups

* NSX and VM-Series Integration: NSX Integration Guide

Q29. Which two deployment modes of VM-Series firewalls are supported across NSX-T? (Choose two.)

* Prism Central
* Service Cluster
* Host-based
* Bootstrap

Service Cluster Mode:

* In NSX-T, the Service Cluster mode allows the VM-Series firewalls to be deployed as part of a service cluster, where they can provide security services to workloads.

Q30. Why are containers uniquely suitable for runtime security based on allow lists?
* Containers have only a few defined processes that should ever be executed.
* Docker has a built-in runtime analysis capability to aid in allow listing.
* Operations teams know which processes are used within a container.
* Developers define the processes used in containers within the Dockerfile.

Containers are typically designed to run a specific application or service, meaning they have a limited and well-defined set of processes. This makes it easier to implement and manage runtime security based on allow lists, as any deviation from the expected processes can be quickly identified and mitigated.

Reference: Security best practices for container environments emphasize the use of allow lists to enforce runtime security, leveraging the predictable nature of container processes.

Palo Alto Networks Container Security Guide

Q31. Which two methods of Zero Trust implementation can benefit an organization? (Choose two.)
* Boundaries are established.
* Security automation is seamlessly integrated.
* Compliance is validated.
* Access controls are enforced.

Zero Trust implementation revolves around the principle that no entity, inside or outside the network, should be trusted by default. The primary methods that benefit an organization are:

* Security automation is seamlessly integrated: Zero Trust requires continuous monitoring and verification of every device and user attempting to access resources. Automation helps in efficiently managing these processes, ensuring that security policies are consistently enforced without human error.

Automated tools can quickly detect anomalies, respond to threats, and update access controls dynamically.

Q32. 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?
* Floating IP address
* VRRP
* ARP load sharing
* HSRP

When implementing active-active high availability (HA), a floating IP address 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. This floating IP address ensures that either of the active-active firewalls can assume control of the traffic without interruption in case of a failover.

References:

* Palo Alto Networks High Availability Guide: Active-Active HA Configuration

* Palo Alto Networks HA Configuration: HA Configuration

Q33. Which three NSX features can be pushed from Panorama in PAN-OS? (Choose three.)
* Multiple authorization codes
* User IP mappings
* Steering rules
* Security group assignment of virtual machines (VMs)

* Security groups
User IP mappings:

* Panorama can push user-to-IP mapping information to the NSX manager, enabling dynamic security policy enforcement based on user identity.

Q34. Which component can provide application-based segmentation and prevent lateral threat movement?
* DNS Security
* NAT
* App-ID *
* URL Filtering
App-ID is a feature that provides application-based segmentation and helps prevent lateral threat movement within a network. By identifying and controlling applications traversing the network regardless of port, protocol, or encryption (SSL or SSH), App-ID allows granular security policies to be applied, thereby limiting the spread of threats within the network.

References:

* Palo Alto Networks App-ID Technology: App-ID

* Palo Alto Networks Application and Threat Content: App-ID Overview

Q35. What do tags allow a VM-Series firewall to do in a virtual environment?
* Integrate with security information and event management (SIEM) solutions.
* Enable machine learning (ML).
* Provide adaptive reporting.
* Adapt Security policy rules dynamically.
Tags in a VM-Series firewall environment allow administrators to dynamically adjust security policy rules based on changes within the virtual environment. These tags can be used to label and categorize virtual machines (VMs) or other entities within the environment, and policies can be created to automatically respond to these tags. This facilitates adaptive security measures that align with the current state and requirements of the environment.

References:

* Palo Alto Networks VM-Series Deployment Guide: Dynamic Address Groups and Tags

Q36. Which two valid components are used in installation of a VM-Series firewall in an OpenStack environment?

(Choose two.)
* VM-Series VHD image
* OpenStack heat template in JSON format
* VM-Series qcow2 image
* OpenStack heat template in YAML Ain’t Markup Language (YAML) format
VM-Series qcow2 image:

* The qcow2 image format is commonly used in OpenStack environments. The VM-Series firewalls are provided in the qcow2 format for compatibility with OpenStack.

Q37. How is traffic directed to a Palo Alto Networks firewall integrated with Cisco ACI?
* Through a policy-based redirect (PBR)
* By creating an access policy

* By using contracts between endpoint groups that send traffic to the firewall using a shared policy
* Through a virtual machine (VM) monitor domain

In Cisco ACI, traffic is directed to a Palo Alto Networks firewall by creating contracts between endpoint groups (EPGs) that send traffic to the firewall. These contracts define the policy for communication between EPGs, ensuring that traffic is inspected and secured by the firewall before reaching its destination.

References:

* Cisco ACI and Palo Alto Networks Integration Guide: Contracts and Policies

* Cisco ACI Fundamentals: ACI Contracts

Q38. With which two private cloud environments does Palo Alto Networks have deep integrations? (Choose two.)
* Cisco ACI
* VMware NSX-T
* Nutanix
* Dell APEX

Palo Alto Networks has deep integrations with:

* Cisco ACI:Integration with Cisco Application Centric Infrastructure (ACI) allows for automated security provisioning and enforcement within the Cisco data center environment, leveraging the tight coupling of network and security policies.

* VMware NSX-T:Integration with VMware NSX-T enables advanced security features and visibility within VMware’s software-defined data center (SDDC) environment, facilitating automated security policies and enforcement across virtualized workloads.

References:

* Palo Alto Networks Integration with Cisco ACI: Cisco ACI Integration

* Palo Alto Networks Integration with VMware NSX-T: VMware NSX-T Integration

Q39. Which offering inspects encrypted outbound traffic?
* TLS decryption
* WildFire
* Content-ID
* Advanced URL Filtering (AURLF)

Q40. What does the number of required flex credits for a VM-Series firewall depend on?
* IP address allocation
* Memory allocation
* Network interface allocation
* vCPU allocation

The number of required flex credits for a VM-Series firewall primarily depends on the vCPU allocation. Flex credits are used to license VM-Series firewalls, and the number of credits required is determined by the number of virtual CPUs (vCPUs) allocated to the firewall. Higher vCPU allocations provide greater performance capabilities and thus require more flex credits.

References:

* Palo Alto Networks Licensing Guide: VM-Series Licensing

* Palo Alto Networks VM-Series Datasheet: VM-Series Datasheet

Q41. Which component scans for threats in allowed traffic?
* Security profiles
* NAT
* Intelligent Traffic Offload
* TLS decryption
* Security Profiles:

* Security profiles in Palo Alto Networks firewalls are used to scan for threats in allowed traffic.

These profiles include features such as Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, and others that inspect traffic and detect potential threats.

Q42. Which two mechanisms could trigger a high availability (HA) failover event? (Choose two.)
* Ping monitoring
* Link monitoring
* Session polling
* Heartbeat polling
Ping monitoring:

* This mechanism involves monitoring the reachability of a specified IP address. If the firewall cannot ping the address, it may trigger a failover.

Q43. Which two elements of the Palo Alto Networks platform architecture enable security orchestration in a software-defined network (SDN)? (Choose two.)
* NVGRE support for advanced VLAN integration
* Full set of APIs enabling programmatic control of policy and configuration
* VXLAN support for network-layer abstraction
* Dynamic Address Groups to adapt Security policies dynamically
Full set of APIs enabling programmatic control of policy and configuration:

* Palo Alto Networks provides a comprehensive set of APIs that allow for the automation and orchestration of security policies and configurations in an SDN environment.

Q44. Which Palo Alto Networks firewall provides network security when deploying a microservices-based application?
* VM-Series
* PA-Series
* HA-Series
* CN-Series
* The CN-Series firewalls are specifically designed to secure Kubernetes and containerized environments, making them ideal for protecting microservices-based applications. They provide network security by integrating directly with the container orchestration platform.

Q45. A CN-Series firewall can secure traffic between which elements?
* Host containers
* Containers
* Pods
* Source applications

The CN-Series firewalls are specifically designed to secure containerized environments. They can secure traffic between Kubernetes pods, which are the smallest deployable units in a Kubernetes cluster, and are often composed of one or more containers. The primary focus of CN-Series firewalls is to ensure security within Kubernetes environments by managing traffic and enforcing security policies at the pod level.

References:

* Palo Alto Networks CN-Series Datasheet: CN-Series Datasheet

* Palo Alto Networks CN-Series Documentation: CN-Series Documentation

Q46. 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?
* HA-Series
* VM-Series
* PA-Series
* CN-Series
VM-Series Auto Scaling:

* The VM-Series firewalls are designed to integrate with cloud environments like AWS and support auto-scaling. This allows for the deployment of a single auto-scaling group (ASG) of VM-Series firewalls to secure inbound traffic from the internet to AWS application workloads.

Q47. How must a Palo Alto Networks Next-Generation Firewall (NGFW) be configured in order to secure traffic in a Cisco ACI environment?
* It must be deployed as a member of a device cluster.
* It must be identified as a default gateway.
* It must receive all forwarding lookups from the network controller.
* It must use a Layer 3 underlay network.
The Palo Alto Networks Next-Generation Firewall must be integrated into the Layer 3 underlay network to secure traffic within a Cisco ACI environment.

Reference: Integration documentation for Cisco ACI and Palo Alto Networks indicates the necessity of Layer

3 integration for policy enforcement and traffic management.

Palo Alto Networks and Cisco ACI Integration