Number: PSE-SoftwareFirewall
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: PSE-SoftwareFirewall

Exam Name: Palo Alto Networks Systems Engineer (PSE): Software Firewall Professional

Exam A

QUESTION 1
What is a benefit of network runtime security?

A. It removes vulnerabilities that have been baked into containers.
B. It more narrowly focuses on one security area and requires careful customization, integration, and maintenance.
C. It is siloed to enhance workload security.
D. It identifies unknown vulnerabilities that cannot be identified by known Common Vulnerability and Exposure (CVE) lists.

Correct Answer: D
Section:
Explanation:
Identifying Unknown Vulnerabilities:
Network runtime security is beneficial because it can identify unknown vulnerabilities that are not listed in known CVE lists. This type of security focuses on monitoring the behavior of applications and containers in real-time, which helps detect anomalies and potential threats that static analysis might miss.
Palo Alto Networks Runtime Security Guide

QUESTION 2
How does Prisma Cloud Compute offer workload security at runtime?

A. It quarantines containers that demonstrate increased CPU and memory usage.
B. It automatically patches vulnerabilities and compliance issues for every container and service.
C. It works with the identity provider (IdP) to identify overprivileged containers and services, and it restricts network access.
D. It automatically builds an allow-list security model for every container and service.

Correct Answer: D
Section:
Explanation:
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.
Prisma Cloud Compute Runtime Security

QUESTION 3
Which type of group allows sharing cloud-learned tags with on-premises firewalls?

A. Notify *
B. Address
C. Template
D. Device

Correct Answer: B
Section:
Explanation:

Address Group:
Address groups in Palo Alto Networks firewalls allow for the grouping of multiple addresses or address objects. This capability enables the sharing of cloud-learned tags with on-premises firewalls, facilitating the consistent application of security policies across hybrid cloud environments.
Palo Alto Networks Address Objects Documentation

QUESTION 4
Which two actions can be performed for VM-Series firewall licensing by an orchestration system? (Choose two.)

A. Registering an authorization code
B. Creating a license
C. Downloading a content update
D. Renewing a license

Correct Answer: A, C
Section:
Explanation:
Registering an Authorization Code:
An orchestration system can automate the registration of authorization codes, which is a critical step in licensing the VM-Series firewall. This process involves submitting the code to Palo Alto Networks to activate the license.
Palo Alto Networks VM-Series Licensing Guide
Downloading a Content Update:
Orchestration systems can also automate the downloading of content updates, which include the latest threat intelligence and security updates. This ensures the firewall remains up-to-date with the latest security information.
Palo Alto Networks Content Updates

QUESTION 5
How is traffic directed to a Palo Alto Networks firewall integrated with Cisco ACI?

A. Through a policy-based redirect (PBR)
B. By creating an access policy
C. By using contracts between endpoint groups that send traffic to the firewall using a shared policy
D. Through a virtual machine (VM) monitor domain

Correct Answer: C
Section:
Explanation:
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.
Cisco ACI and Palo Alto Networks Integration Guide: Contracts and Policies
Cisco ACI Fundamentals: ACI Contracts

QUESTION 6
Which PAN-OS feature allows for automated updates to address objects when VM-Series firewalls are setup as part of an NSX deployment?

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

Correct Answer: A
Section:
Explanation:
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.
Palo Alto Networks Dynamic Address Groups: Dynamic Address Groups
NSX and VM-Series Integration: NSX Integration Guide

QUESTION 7
Which component scans for threats in allowed traffic?

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

Correct Answer: A
Section:
Explanation:
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.
Palo Alto Networks Security Profiles

QUESTION 8
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. Traditional active-active HA
B. Transit gateway and Security VPC
C. Traditional active-passive HA
D. Transit VPC and Security VPC

Correct Answer: B, D
Section:
Explanation:
Transit Gateway and Security VPC:
Using a transit gateway in conjunction with a Security VPC is a recommended design for outbound high availability (HA) in AWS. This configuration ensures that traffic can be routed efficiently and securely through the VM-Series firewalls deployed in the Security VPC.
Palo Alto Networks AWS Design Guide
Transit VPC and Security VPC:
Another recommended approach is to use a Transit VPC along with a Security VPC. The Transit VPC provides a centralized routing hub, while the Security VPC hosts the VM-Series firewalls to inspect and secure outbound traffic.
Palo Alto Networks AWS Transit VPC Guide

QUESTION 9
How are Palo Alto Networks Next-Generation Firewalls (NGFWs) deployed within a Cisco ACI architecture?

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

B. VXLAN or NVGRE traffic is terminated and inspected for translation to VLANs.
C. Service graphs are configured to allow their deployment.
D. SDN code hooks can help detonate malicious file samples designed to detect virtual environments.

Correct Answer: C
Section:
Explanation:
Within a Cisco ACI architecture, Palo Alto Networks Next-Generation Firewalls (NGFWs) are deployed using service graphs. Service graphs in Cisco ACI define the sequence of network services that traffic must pass through. By configuring service graphs, administrators can seamlessly integrate Palo Alto Networks firewalls into the fabric to inspect and secure traffic flows.
Palo Alto Networks and Cisco ACI Integration Guide: Service Graphs Integration
Cisco ACI Service Graph Documentation: Service Graphs

QUESTION 10
Which two factors lead to improved return on investment for prospects interested in Palo Alto Networks virtualized next-generation firewalls (NGFWs)? (Choose two.)

A. Reduced operational expenditures
B. Decreased likelihood of data breach
C. Reduced insurance premiums
D. Reduced time to deploy

Correct Answer: A, D
Section:
Explanation:
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.
Reduced time to deploy: Virtual NGFWs can be quickly deployed in various environments, such as public clouds or virtualized data centers, compared to the time-consuming process of installing physical hardware. This agility allows organizations to respond faster to security needs and market demands.

QUESTION 11
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. Dynamic address group
D. App-ID

Correct Answer: C
Section:
Explanation:
Dynamic address groups in Palo Alto Networks firewalls provide flexibility by allowing network resources to be added without requiring changes to existing policies and rules:
Dynamic address group: These groups automatically update based on tags and attributes assigned to network objects. When new resources are added with the appropriate tags, they are dynamically included in the address group, and the associated policies automatically apply to them without manual intervention.

QUESTION 12
Which software firewall would help a prospect interested in securing an environment with Kubernetes?

A. ML-Series
B. CN-Series
C. KN-Series
D. VM-Series

Correct Answer: B
Section:
Explanation:
The CN-Series firewalls are purpose-built for securing Kubernetes environments. They provide network security, visibility, and threat prevention specifically tailored to containerized applications and microservices running in Kubernetes.
Palo Alto Networks CN-Series Overview

QUESTION 13
Which two design options address split brain when configuring high availability (HA)? (Choose two.)

A. Bundling multiple interfaces in an aggregated interface group and assigning HA2
B. Using the heartbeat backup
C. Sending heartbeats across the HA2 interfaces
D. Adding a backup HA1 interface

Correct Answer: B, D
Section:
Explanation:
Using the Heartbeat Backup:
The heartbeat backup is a mechanism that helps to prevent split-brain scenarios in a high availability (HA) configuration by providing an additional path for heartbeat communication. This ensures that both firewalls in the HA pair are aware of each other's status.
Palo Alto Networks HA Configuration Guide
Adding a Backup HA1 Interface:
Configuring a backup HA1 interface provides redundancy for the primary HA1 link, ensuring continued communication between HA peers even if the primary link fails. This setup is crucial for maintaining synchronization and preventing split-brain scenarios.
Palo Alto Networks HA Configuration

QUESTION 14
How are CN-Series firewalls licensed?

A. Management-plane vCPU
B. Data-plane vCPU
C. Control-plane vCPU
D. Service-plane vCPU

Correct Answer: B
Section:
Explanation:
Data-plane vCPU Licensing:
The CN-Series firewalls are licensed based on the number of data-plane vCPUs. This licensing model reflects the processing power dedicated to handling traffic and security enforcement within the containerized environment.
Palo Alto Networks CN-Series Licensing Guide

QUESTION 15

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

A. Environment/Kubernetes/Deployment_Type
B. Kubernetes/Environment/Deployment_Type
C. Deployment_Type/Kubernetes/Environment
D. Kubernetes/Deployment_Type/Environment

Correct Answer: D
Section:
Explanation:
YAML File Structure:
The structure of a YAML file repository for managing configurations typically follows the order of Kubernetes/Deployment_Type/Environment. This hierarchy ensures that the configurations are organized logically, with Kubernetes-specific settings at the top level, followed by the type of deployment, and then the specific environment.
Kubernetes YAML Best Practices

QUESTION 16
Which solution is best for securing an EKS environment?

A. API orchestration
B. CN-Series high availability (HA) pair
C. PA-Series using load sharing
D. VM-Series single host

Correct Answer: B
Section:
Explanation:
CN-Series for EKS Security:
The CN-Series firewalls are specifically designed to secure Kubernetes environments, such as Amazon EKS. Deploying them in a high availability (HA) pair ensures robust, fault-tolerant security for containerized workloads, providing continuous protection and high availability.
Palo Alto Networks CN-Series Deployment Guide

QUESTION 17
A CN-Series firewall can secure traffic between which elements?

A. Host containers
B. Containers
C. Pods
D. Source applications

Correct Answer: C
Section:
Explanation:
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.
Palo Alto Networks CN-Series Datasheet: CN-Series Datasheet
Palo Alto Networks CN-Series Documentation: CN-Series Documentation

QUESTION 18

What Palo Alto Networks software firewall protects Amazon Web Services (AWS) deployments with network security delivered as a managed cloud service?

A. Ion-Series Ion-Series
B. CN-Series
C. Cloud next-generation firewall (NGFW)
D. VM-Series

Correct Answer: C
Section:
Explanation:
The Cloud NGFW by Palo Alto Networks is a managed cloud service designed to provide advanced network security capabilities within AWS deployments. This service leverages Palo Alto Networks' technology to deliver scalable and comprehensive security without the need for users to manage the infrastructure themselves. It is ideal for organizations looking to integrate robust security within their cloud environments efficiently.
Palo Alto Networks Cloud NGFW for AWS: Cloud NGFW for AWS
AWS Marketplace: Cloud NGFW for AWS

QUESTION 19
Which protocol is used for communicating between VM-Series firewalls and a gateway load balancer in Amazon Web Services (AWS)?

A. Geneve
B. VRLAN
C. VMLAN
D. GRE

Correct Answer: A
Section:
Explanation:
Geneve (Generic Network Virtualization Encapsulation) is the protocol used for communication between VM-Series firewalls and a Gateway Load Balancer (GWLB) in AWS. Geneve provides a flexible encapsulation method and is specifically supported for integrating with AWS GWLB to ensure seamless traffic flow and security inspection.
AWS Gateway Load Balancer Documentation: AWS GWLB
Palo Alto Networks Integration Guide: Integrating VM-Series with AWS GWLB

QUESTION 20
Which two routing options are supported by VM-Series? (Choose two.)

A. RIP
B. OSPF
C. IGRP
D. BGP

Correct Answer: B, D
Section:
Explanation:
The VM-Series firewalls support various dynamic routing protocols to ensure efficient and resilient network traffic management. Among these, OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) are supported. OSPF is used for intra-domain routing, while BGP is essential for inter-domain routing, allowing VM-Series to participate in complex and scalable network topologies.
Palo Alto Networks VM-Series Deployment Guide: VM-Series Deployment Guide
Palo Alto Networks Administrator's Guide: Routing Protocols

QUESTION 21

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
Section:
Explanation:
VM-Series firewalls provide advanced application-level security for web-server instances on AWS. These virtual firewalls leverage Palo Alto Networks' next-generation firewall capabilities to offer features like application identification, threat prevention, and URL filtering, ensuring comprehensive security for web applications hosted on AWS.
Palo Alto Networks VM-Series on AWS: VM-Series on AWS
AWS Security Best Practices: AWS Security Best Practices

QUESTION 22
Which two valid components are used in installation of a VM-Series firewall in an OpenStack environment? (Choose two.)

A. VM-Series VHD image
B. OpenStack heat template in JSON format
C. VM-Series qcow2 image
D. OpenStack heat template in YAML Ain't Markup Language (YAML) format

Correct Answer: C, D
Section:
Explanation:
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.
Palo Alto Networks VM-Series Deployment Guide
OpenStack heat template in YAML format:
OpenStack Heat Orchestration Templates (HOT) are written in YAML. These templates define the infrastructure needed for deployment and can automate the deployment process.
OpenStack Heat Documentation

QUESTION 23
Which three NSX features can be pushed from Panorama in PAN-OS? (Choose three.)

A. Multiple authorization codes
B. User IP mappings
C. Steering rules
D. Security group assignment of virtual machines (VMs)
E. Security groups

Correct Answer: B, C, D
Section:
Explanation:
User IP mappings:
Panorama can push user-to-IP mapping information to the NSX manager, enabling dynamic security policy enforcement based on user identity.
PAN-OS NSX Integration Guide

Steering rules:
Steering rules dictate how traffic is directed through security services. Panorama can push these rules to ensure traffic is properly inspected.
Palo Alto Networks NSX Integration
Security group assignment of virtual machines (VMs):
Panorama can push security group information, ensuring that VMs are dynamically assigned to the appropriate security policies.
Palo Alto Networks NSX Integration Guide

QUESTION 24
Which two mechanisms could trigger a high availability (HA) failover event? (Choose two.)

A. Ping monitoring
B. Link monitoring
C. Session polling
D. Heartbeat polling

Correct Answer: A, B
Section:
Explanation:
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.
PAN-OS Administrator's Guide - HA
Link monitoring:
Link monitoring checks the status of network links. If a monitored link fails, an HA failover can be triggered.
PAN-OS High Availability Link Monitoring

QUESTION 25
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 be identified as a default gateway.
C. It must receive all forwarding lookups from the network controller.
D. It must use a Layer 3 underlay network.

Correct Answer: D
Section:
Explanation:
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

QUESTION 26
Which two elements of the Palo Alto Networks platform architecture enable security orchestration in a software-defined network (SDN)? (Choose two.)

A. NVGRE support for advanced VLAN integration
B. Full set of APIs enabling programmatic control of policy and configuration
C. VXLAN support for network-layer abstraction
D. Dynamic Address Groups to adapt Security policies dynamically

Correct Answer: B, D
Section:
Explanation:
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.
PAN-OS API Guide
Dynamic Address Groups to adapt Security policies dynamically:
Dynamic Address Groups (DAGs) enable the firewall to automatically adjust policies based on dynamic conditions, crucial for SDN environments where network configurations frequently change.
Dynamic Address Groups - PAN-OS

QUESTION 27
What do tags allow a VM-Series firewall to do in a virtual environment?

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

Correct Answer: D
Section:
Explanation:
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.
Palo Alto Networks VM-Series Deployment Guide: Dynamic Address Groups and Tags

QUESTION 28
Which two criteria are required to deploy VM-Series firewalls in high availability (HA)? (Choose two.)

A. Configuration of asymmetric routing
B. Assignment of identical licenses and subscriptions
C. Deployment on a different host
D. Deployment on same type of hypervisor

Correct Answer: B, D
Section:
Explanation:
For deploying VM-Series firewalls in high availability (HA), it is crucial to ensure that both firewalls in the HA pair have identical licenses and subscriptions to ensure feature parity and uninterrupted service during failover. Additionally, both firewalls must be deployed on the same type of hypervisor to ensure compatibility and proper synchronization of state and configurations between the active and passive units.
Palo Alto Networks High Availability Guide: HA Requirements
Palo Alto Networks VM-Series Deployment Guide: High Availability

QUESTION 29
What can software next-generation firewall (NGFW) credits be used to provision?

A. Enablement of DNS security
B. Virtual Panorama appliances
C. Remote browser isolation

D. Migrating NGFWs from hardware to VMs

Correct Answer: A
Section:
Explanation:
Software next-generation firewall (NGFW) credits can be used to enable DNS security on Palo Alto Networks firewalls. These credits allow customers to activate DNS Security service, which provides real-time protection against DNS-based threats by leveraging machine learning and continuous analysis.
Palo Alto Networks DNS Security: DNS Security
Palo Alto Networks Licensing Guide: Software NGFW Credits

QUESTION 30
What is required to integrate a Palo Alto Networks VM-Series firewall with Azure Orchestration?

A. Client-ID
B. API Key
C. Dynamic Address Groups
D. Aperture orchestration engine

Correct Answer: B
Section:
Explanation:
To integrate a Palo Alto Networks VM-Series firewall with Azure Orchestration, an API Key is required. The API Key is used to authenticate and authorize the firewall to interact with Azure services, enabling automated management and orchestration of security policies and configurations.
Palo Alto Networks Integration with Azure: Azure Integration
Azure API Management: Azure API Key

QUESTION 31
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 the Config tab, then select New Route from the Security Zone Route drop-down menu.
C. Select Network > Interfaces.
D. Select Network > Virtual Router, then select the default link to open the Virtual Router dialog.

Correct Answer: A, D
Section:
Explanation:
To configure a default route to an internet router, you need to perform the following steps:
Select Network > Virtual Router, then select the default link to open the Virtual Router dialog.
Select the Static Routes tab, then click Add to create a new static route.
These steps ensure that the default route is correctly added to the virtual router configuration, allowing traffic to be directed to the appropriate internet gateway.
Palo Alto Networks Configuration Guide: Configuring Default Route
Palo Alto Networks Virtual Router Configuration: Virtual Router

QUESTION 32
Which two steps are involved in deployment of a VM-Series firewall on NSX? (Choose two.)

A. Create a virtual data center (vDC) and a vApp that includes the VM-Series firewall.

B. Enable communication between Panorama and the NSX Manager.
C. Register the VM-Series firewall as a service.
D. Obtain the Amazon Machine Images (AMIs) from marketplace.

Correct Answer: B, C
Section:
Explanation:
This step involves setting up a connection between Panorama (the centralized management platform for Palo Alto Networks firewalls) and the VMware NSX Manager. This communication is essential for managing and orchestrating the VM-Series firewalls within the NSX environment.
Palo Alto Networks VMware NSX Integration Guide
Register the VM-Series firewall as a service:
Registering the VM-Series firewall as a service in the NSX Manager is crucial for the firewall to be recognized and managed within the NSX environment. This step allows the firewall to be deployed and configured as part of the NSX service chaining.
Palo Alto Networks VMware NSX Integration Guide

QUESTION 33
Why are VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster problematic for protecting containerized workloads?

A. They function differently based on whether they are located inside or outside of the cluster.
B. They are located outside the cluster and have no visibility into application-level cluster traffic.
C. They are managed by another entity when located inside the cluster.
D. They do not scale independently of the Kubernetes cluster.

Correct Answer: B
Section:
Explanation:
Visibility into application-level cluster traffic:
VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster lack the necessary visibility into the traffic and communications occurring at the application level within the cluster. This limitation impedes their ability to effectively protect containerized workloads.
Palo Alto Networks Kubernetes Security Guide

QUESTION 34
What are two environments supported by the CN-Series firewall? (Choose two.)

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

Correct Answer: A, C
Section:
Explanation:
OpenShift:
The CN-Series firewall supports deployment in Red Hat OpenShift environments. OpenShift is a Kubernetes-based container platform that provides a comprehensive solution for container orchestration.
Palo Alto Networks CN-Series Deployment Guide
Native K8:
The CN-Series firewall is designed to be deployed in native Kubernetes (K8s) environments, providing security for containerized applications running within the Kubernetes clusters.
Palo Alto Networks CN-Series Deployment Guide

QUESTION 35
Which software firewall would assist a prospect who is interested in securing extensive DevOps deployments?

A. VM-Series
B. CN-Series
C. Ion-Series
D. Cloud next-generation firewall (NGFW)

Correct Answer: B
Section:
Explanation:
CN-Series for DevOps deployments:
The CN-Series firewall is specifically designed to secure containerized environments and is ideal for protecting extensive DevOps deployments. It integrates seamlessly with Kubernetes and other container orchestration platforms, providing the necessary security controls for DevOps processes.
Palo Alto Networks CN-Series Firewall Overview

QUESTION 36
Which two features of CN-Series firewalls protect east-west traffic between pods in different trust zones? (Choose two.)

A. Intrusion prevention system (IPS)
B. Communication with Panorama
C. External load balancer (ELB)
D. Layer 7 visibility

Correct Answer: A, D
Section:
Explanation:
Intrusion Prevention System (IPS): The CN-Series firewalls incorporate an Intrusion Prevention System to detect and prevent exploits and attacks on applications and systems. This feature is essential for securing east-west traffic, as it can identify and block threats within the data center traffic between pods in different trust zones.
Layer 7 Visibility: CN-Series firewalls provide Layer 7 (application layer) visibility, enabling deep inspection of application traffic. This allows the firewall to understand and enforce policies based on the application and its behavior, rather than just ports and protocols, ensuring comprehensive security for east-west traffic within a Kubernetes environment.
Palo Alto Networks CN-Series Datasheet: CN-Series Datasheet
Palo Alto Networks CN-Series Documentation: CN-Series Documentation

QUESTION 37
Which technology allows for granular control of east-west traffic in a software-defined network?

A. Microsegmentation
B. MAC Access Control List
C. Routing
D. Virtualization

Correct Answer: A
Section:
Explanation:
Microsegmentation is a security technique that enables granular control of east-west traffic within a software-defined network. By dividing the network into smaller segments, each with its own security policies, microsegmentation allows for detailed control over communication between workloads, thereby reducing the attack surface and preventing lateral movement of threats within the network.
Palo Alto Networks Microsegmentation Guide: Microsegmentation Guide

VMware NSX Microsegmentation: NSX Microsegmentation

QUESTION 38
With which two private cloud environments does Palo Alto Networks have deep integrations? (Choose two.)

A. Cisco ACI
B. VMware NSX-T
C. Nutanix
D. Dell APEX

Correct Answer: A, B
Section:
Explanation:
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.
Palo Alto Networks Integration with Cisco ACI: Cisco ACI Integration
Palo Alto Networks Integration with VMware NSX-T: VMware NSX-T Integration

QUESTION 39
Which two public cloud platforms does the VM-Series plugin support? (Choose two.)

A. IBM Cloud
B. OCI
C. Amazon Web Services (AWS)
D. Azure

Correct Answer: C, D
Section:
Explanation:
The VM-Series plugin supports integration with multiple public cloud platforms, including:
Amazon Web Services (AWS): The VM-Series firewalls can be deployed in AWS to provide comprehensive security for cloud applications and data, leveraging AWS's native services and integration capabilities.
Azure: The VM-Series firewalls also integrate with Microsoft Azure, offering advanced security features and policies for applications and data hosted in Azure's cloud environment.
Palo Alto Networks VM-Series on AWS: VM-Series on AWS
Palo Alto Networks VM-Series on Azure: VM-Series on Azure

QUESTION 40
How does a CN-Series firewall prevent exfiltration?

A. It distributes incoming virtual private cloud (VPC) traffic across the pool of VM-Series firewalls.
B. It inspects outbound traffic content and blocks suspicious activity.
C. It provides a license deactivation API key.
D. It employs custom-built signatures based on hash.

Correct Answer: C
Section:

Explanation:
The CN-Series firewall prevents data exfiltration by inspecting the content of outbound traffic. It uses advanced security features, such as threat prevention and data loss prevention (DLP), to detect and block suspicious activities and unauthorized data transfers, ensuring sensitive data remains within the secure environment.
Palo Alto Networks CN-Series Documentation: CN-Series Documentation
Palo Alto Networks Threat Prevention: Threat Prevention

QUESTION 41
What is a benefit of CN-Series firewalls securing traffic between pods and other workload types?

A. It allows for automatic deployment, provisioning, and immediate policy enforcement without any manual intervention.
B. It ensures consistent security across the entire environment.
C. It allows extension of Zero Trust Network Security to the most remote locations and smallest branches.
D. It protects data center and internet gateway deployments.

Correct Answer: B
Section:
Explanation:
Consistent Security Across the Environment:
CN-Series firewalls are designed to provide security for containerized environments by protecting traffic between pods and other workload types. This ensures that security policies are consistently enforced across all elements of the environment, maintaining a unified security posture.
Palo Alto Networks CN-Series Documentation

QUESTION 42
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.)

A. Threat Prevention
B. SD-WAN
C. Intelligent Traffic Offload
D. WildFire

Correct Answer: A, D
Section:
Explanation:
For a customer deploying VM-Series firewalls in a private data center and concerned about protecting resources from malware and lateral movement, the following subscriptions are recommended:
Threat Prevention: This subscription provides comprehensive threat detection and prevention capabilities, including IPS, anti-virus, anti-spyware, and vulnerability protection.
WildFire: This advanced threat intelligence service analyzes suspicious files and identifies new malware, providing protection against zero-day exploits and threats.
Palo Alto Networks Threat Prevention: Threat Prevention
Palo Alto Networks WildFire: WildFire

QUESTION 43
Which two methods of Zero Trust implementation can benefit an organization? (Choose two.)

A. Boundaries are established.
B. Security automation is seamlessly integrated.
C. Compliance is validated.
D. Access controls are enforced.

Correct Answer: B, D
Section:
Explanation:
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.
Access controls are enforced: Zero Trust models implement strict access controls based on the principle of least privilege. This means users and devices are given the minimum levels of access -- or permissions -- necessary to perform their jobs. Enforcing access controls ensures that only authenticated and authorized entities can access specific resources.

QUESTION 44
What is the appropriate file format for Kubernetes applications?

A. .yaml
B. .exe
C. Json
D. .xml

Correct Answer: A
Section:
Explanation:
In Kubernetes, configuration files are typically written in YAML (.yaml) format. YAML (Yet Another Markup Language) is preferred due to its readability and ease of use for defining complex data structures like those required for Kubernetes deployments. Kubernetes uses these YAML files to define resources such as pods, services, and deployments.
Kubernetes Documentation on YAML: Kubernetes YAML
Kubernetes Getting Started Guide: YAML Basics