Number: PSE-SWFW-Pro-24
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: PSE-SWFW-Pro-24

Exam Name: Palo Alto Networks Systems Engineer Professional - Software Firewall

Exam A

QUESTION 1
A company is sponsoring a cybersecurity conference for attendees interested in a range of cybersecurity products that include malware protection, SASE, automation products, and firewalls. The company will deliver a single 3--4 hour conference workshop.
Which cybersecurity portfolio tool will give workshop attendees the appropriate exposure to the widest variety of Palo Alto Networks products?

A. Capture the Flag
B. Ultimate Lab Environment
C. Demo Environment
D. Ultimate Test Drive

Correct Answer: B
Section:
Explanation:
For a conference workshop showcasing a wide range of Palo Alto Networks products, the Ultimate Lab Environment is the most suitable option.
A . Capture the Flag: CTFs are interactive security competitions focusing on specific vulnerabilities and exploits. While engaging, they don't provide broad exposure to the full product portfolio.
B . Ultimate Lab Environment: This environment is designed to provide hands-on experience with various Palo Alto Networks products and solutions, including firewalls, Prisma Access (SASE), Cortex (automation), and more. It's ideal for demonstrating the integrated platform and diverse capabilities.
C . Demo Environment: While demo environments showcase product features, they are typically pre-configured and lack the interactive, hands-on experience of a lab environment.
D . Ultimate Test Drive: Test Drives focus on specific use cases or products, not the breadth of the entire portfolio.

QUESTION 2
Which three tools or methods automate VM-Series firewall deployment? (Choose three.)

A. Panorama Software Firewall License plugin
B. Palo Alto Networks GitHub repository
C. Bootstrap the VM-Series firewall
D. Shared Disk Software Library folder
E. Panorama Software Library image

Correct Answer: B, C, E
Section:
Explanation:
Several tools and methods automate VM-Series firewall deployment:
A . Panorama Software Firewall License plugin: Panorama is used for managing firewalls, not directly for automating their initial deployment.
B . Palo Alto Networks GitHub repository: Palo Alto Networks maintains repositories on GitHub containing Terraform modules, Ansible playbooks, and other automation tools for deploying VM-Series firewalls in various cloud and on-premises environments.
C . Bootstrap the VM-Series firewall: Bootstrapping allows for automated initial configuration of the VM-Series firewall using a configuration file stored on a cloud storage service (like S3 or Azure Blob Storage). This automates initial setup tasks like setting the management IP and retrieving licenses.
D . Shared Disk Software Library folder: This is not a standard method for automating VM-Series deployment.
E . Panorama Software Library image: While Panorama doesn't directly deploy the VM-Series instance, using a pre-configured Software Library image within Panorama can automate much of the post-deployment configuration and management, effectively streamlining the overall deployment process.
VM-Series Deployment Guides: These guides detail bootstrapping and often reference automation tools on GitHub.
Panorama Administrator's Guide: This explains how to use Software Library images.

These resources confirm that GitHub repositories, bootstrapping, and using Panorama Software Library images are methods for automating VM-Series deployment.

QUESTION 3
Why should a customer use advanced versions of Cloud-Delivered Security Services (CDSS) subscriptions compared to legacy versions when creating or editing a deployment profile?
(e.g., using Advanced Threat Prevention instead of Threat Prevention.)

A. To improve firewall throughput by inspecting hashes of advanced packet headers
B. To download and install new threat-related signature databases in real-time
C. To use cloud-scale machine learning inline for detection of highly evasive and zero-day threats
D. To use external dynamic lists for blocking known malicious threat sources and destinations

Correct Answer: C
Section:
Explanation:
Advanced CDSS subscriptions offer enhanced threat prevention capabilities:
A . To improve firewall throughput by inspecting hashes of advanced packet headers: While some security features use hashing, this is not the primary advantage of advanced CDSS.
B . To download and install new threat-related signature databases in real-time: Both standard and advanced CDSS subscriptions receive regular threat updates.
C . To use cloud-scale machine learning inline for detection of highly evasive and zero-day threats: This is a key differentiator of advanced CDSS. It leverages cloud-based machine learning to detect sophisticated threats that traditional signature-based methods might miss.
D . To use external dynamic lists for blocking known malicious threat sources and destinations: Both standard and advanced CDSS can use external dynamic lists.
Information about the specific features of advanced CDSS, such as inline machine learning, can be found on the Palo Alto Networks website and in datasheets comparing different CDSS subscription levels.

QUESTION 4
Which statement applies when identifying the appropriate Palo Alto Networks firewall platform for virtualized as well as cloud environments?

A. VM-Series firewalls cannot be used to protect container environments.
B. All NGFW platforms support API integration.
C. Panorama is the only unified management console for all NGFWs.
D. CN-Series firewalls are used to protect virtualized environments.

Correct Answer: B
Section:
Explanation:
A . VM-Series firewalls cannot be used to protect container environments: This is incorrect. While CN-Series is specifically designed for container environments, VM-Series can also be used in certain container deployments, often in conjunction with other container networking solutions. For example, VM-Series can be deployed as a gateway for a Kubernetes cluster.
B . All NGFW platforms support API integration: This is correct. Palo Alto Networks firewalls, including PA-Series (hardware), VM-Series (virtualized), CN-Series (containerized), and Cloud NGFW, offer robust API support for automation, integration with other systems, and programmatic management. This is a core feature of their platform approach.
C . Panorama is the only unified management console for all NGFWs: This is incorrect. While Panorama is a powerful centralized management platform, it's not the only option. Individual firewalls can be managed locally via their web interface or CLI. Additionally, Cloud NGFW has its own management interface within the cloud provider's console.
D. CN-Series firewalls are used to protect virtualized environments: This is incorrect. CN-Series is specifically designed for containerized environments (e.g., Kubernetes, OpenShift), not general virtualized environments. VM-Series is the appropriate choice for virtualized environments (e.g., VMware vSphere, AWS EC2).

QUESTION 5
Which capability, as described in the Securing Applications series of design guides for VM-Series firewalls, is common across Azure, GCP, and AWS?

A. BGP dynamic routing to peer with cloud and on-premises routers
B. GlobalProtect portal and gateway services
C. Horizontal scalability through cloud-native load balancers

D. Site-to-site VPN

Correct Answer: C
Section:
Explanation:
The question asks about a capability common to VM-Series deployments across Azure, GCP, and AWS, as described in the 'Securing Applications' design guides.
C . Horizontal scalability through cloud-native load balancers: This is the correct answer. A core concept in cloud deployments, and emphasized in the 'Securing Applications' guides, is using cloud-native load balancers (like Azure Load Balancer, Google Cloud Load Balancing, and AWS Elastic Load Balancing) to distribute traffic across multiple VM-Series firewall instances. This provides horizontal scalability, high availability, and fault tolerance. This is common across all three major cloud providers.
Why other options are incorrect:
A . BGP dynamic routing to peer with cloud and on-premises routers: While BGP is supported by VM-Series and can be used for dynamic routing in cloud environments, it is not explicitly highlighted as a common capability across all three clouds in the 'Securing Applications' guides. The guides focus more on the application security aspects and horizontal scaling. Also, the specific BGP configurations and integrations can differ slightly between cloud providers.
B . GlobalProtect portal and gateway services: While GlobalProtect can be used with VM-Series in cloud environments, the 'Securing Applications' guides primarily focus on securing application traffic within the cloud environment, not remote access. GlobalProtect is more relevant for remote user access or site-to-site VPNs, which are not the primary focus of these guides.
D . Site-to-site VPN: While VM-Series firewalls support site-to-site VPNs in all three clouds, this is not the core focus or common capability highlighted in the 'Securing Applications' guides. These guides emphasize securing application traffic within the cloud using techniques like microsegmentation and horizontal scaling.
Palo Alto Networks
Reference:
The key reference here is the 'Securing Applications' design guides for VM-Series firewalls. These guides are available on the Palo Alto Networks support site (live.paloaltonetworks.com). Searching for 'VM-Series Securing Applications' along with the name of the respective cloud provider (Azure, GCP, AWS) will usually provide the relevant guides

QUESTION 6
A company that purchased software NGFW credits from Palo Alto Networks has made a decision on the number of virtual machines (VMs) and licenses they wish to deploy in AWS cloud.
How are the VM licenses created?

A. Access the AWS Marketplace and use the software NGFW credits to purchase the VMs.
B. Access the Palo Alto Networks Application Hub and create a new VM profile.
C. Access the Palo Alto Networks Customer Support Portal and request the creation of a new software NGFW serial number.
D. Access the Palo Alto Networks Customer Support Portal and create a software NGFW credits deployment profile.

Correct Answer: D
Section:
Explanation:
The question focuses on how VM licenses are created when a company has purchased software NGFW credits and wants to deploy VM-Series firewalls in AWS.
D . Access the Palo Alto Networks Customer Support Portal and create a software NGFW credits deployment profile. This is the correct answer. The process starts in the Palo Alto Networks Customer Support Portal. You create a deployment profile that specifies the number and type of VM-Series licenses you want to deploy. This profile is then used to activate the licenses on the actual VM-Series instances in AWS.
Why other options are incorrect:
A . Access the AWS Marketplace and use the software NGFW credits to purchase the VMs. You do deploy the VM-Series instances from the AWS Marketplace (or through other deployment methods like CloudFormation templates), but you don't 'purchase' the licenses there. The credits are managed separately through the Palo Alto Networks Customer Support Portal. The Marketplace deployment is for the VM instance itself, not the license.
B . Access the Palo Alto Networks Application Hub and create a new VM profile. The Application Hub is not directly involved in the license creation process. It's more focused on application-level security and content updates.
C . Access the Palo Alto Networks Customer Support Portal and request the creation of a new software NGFW serial number. You don't request individual serial numbers for each VM. The deployment profile manages the allocation of licenses from your pool of credits. While each VM will have a serial number once deployed, you don't request them individually during this stage. The deployment profile ties the licenses to the deployment, not individual serial numbers ahead of deployment.
Palo Alto Networks
Reference:
The Palo Alto Networks Customer Support Portal documentation and the VM-Series Deployment Guide are the primary references. Search the support portal (live.paloaltonetworks.com) for 'software NGFW credits,' 'deployment profile,' or 'VM-Series licensing.'
The documentation will describe the following general process:

Purchase software NGFW credits.
Log in to the Palo Alto Networks Customer Support Portal.
Create a deployment profile, specifying the number and type of VM-Series licenses (e.g., VM-Series for AWS, VM-Series for Azure, etc.) you want to allocate from your credits.
Deploy the VM-Series instances in your cloud environment (e.g., from the AWS Marketplace).
Activate the licenses on the VM-Series instances using the deployment profile.
This process confirms that creating a deployment profile in the customer support portal is the correct way to manage and allocate software NGFW licenses.

QUESTION 7
What is the primary purpose of the pan-os-python SDK?

A. To create a Python-based firewall that is compatible with the latest PAN-OS
B. To replace the PAN-OS web interface with a Python-based interface
C. To automate the deployment of PAN-OS firewalls by using Python
D. To provide a Python interface to interact with PAN-OS firewalls and Panorama

Correct Answer: D
Section:
Explanation:
The question asks about the primary purpose of the pan-os-python SDK.
D . To provide a Python interface to interact with PAN-OS firewalls and Panorama: This is the correct answer. The pan-os-python SDK (Software Development Kit) is designed to allow Python scripts and applications to interact programmatically with Palo Alto Networks firewalls (running PAN-OS) and Panorama. It provides functions and classes that simplify tasks like configuration management, monitoring, and automation.
Why other options are incorrect:
A . To create a Python-based firewall that is compatible with the latest PAN-OS: The pan-os-python SDK is not about creating a firewall itself. It's a tool for interacting with existing PAN-OS firewalls.
B . To replace the PAN-OS web interface with a Python-based interface: While you can build custom tools and interfaces using the SDK, its primary purpose is not to replace the web interface. The web interface remains the standard management interface.
C . To automate the deployment of PAN-OS firewalls by using Python: While the SDK can be used as part of an automated deployment process (e.g., in conjunction with tools like Terraform or Ansible), its core purpose is broader: to provide a general Python interface for interacting with PAN-OS and Panorama, not just for deployment.
Palo Alto Networks
Reference:
The primary reference is the official pan-os-python SDK documentation, which can be found on GitHub (usually in the Palo Alto Networks GitHub organization) and is referenced on the Palo Alto Networks Developer portal.
Searching for 'pan-os-python' on the Palo Alto Networks website or on GitHub will locate the official repository.
The documentation will clearly state that the SDK's purpose is to:
Provide a Pythonic way to interact with PAN-OS devices.
Abstract the underlying XML API calls, making it easier to write scripts.
Support various operations, including configuration, monitoring, and operational commands.
The documentation will contain examples demonstrating how to use the SDK to perform various tasks, reinforcing its role as a Python interface for PAN-OS and Panorama.

QUESTION 8
Which use case is valid for Strata Cloud Manager (SCM)?

A. Provisioning and licensing new CN-Series firewall deployments
B. Providing AI-Powered ADEM for all Prisma Access users
C. Supporting pre PAN-OS 10.1 SD-WAN migrations to SCM
D. Providing API-driven plugin framework for integration with third-party ecosystems

Correct Answer: D
Section:
Explanation:
The question asks about the primary purpose of the pan-os-python SDK.

D . To provide a Python interface to interact with PAN-OS firewalls and Panorama: This is the correct answer. The pan-os-python SDK (Software Development Kit) is designed to allow Python scripts and applications to interact programmatically with Palo Alto Networks firewalls (running PAN-OS) and Panorama. It provides functions and classes that simplify tasks like configuration management, monitoring, and automation.
Why other options are incorrect:
A . To create a Python-based firewall that is compatible with the latest PAN-OS: The pan-os-python SDK is not about creating a firewall itself. It's a tool for interacting with existing PAN-OS firewalls.
B . To replace the PAN-OS web interface with a Python-based interface: While you can build custom tools and interfaces using the SDK, its primary purpose is not to replace the web interface. The web interface remains the standard management interface.
C . To automate the deployment of PAN-OS firewalls by using Python: While the SDK can be used as part of an automated deployment process (e.g., in conjunction with tools like Terraform or Ansible), its core purpose is broader: to provide a general Python interface for interacting with PAN-OS and Panorama, not just for deployment.
Palo Alto Networks
Reference:
The primary reference is the official pan-os-python SDK documentation, which can be found on GitHub (usually in the Palo Alto Networks GitHub organization) and is referenced on the Palo Alto Networks Developer portal.
Searching for 'pan-os-python' on the Palo Alto Networks website or on GitHub will locate the official repository.
The documentation will clearly state that the SDK's purpose is to:
Provide a Pythonic way to interact with PAN-OS devices.
Abstract the underlying XML API calls, making it easier to write scripts.
Support various operations, including configuration, monitoring, and operational commands.
The documentation will contain examples demonstrating how to use the SDK to perform various tasks, reinforcing its role as a Python interface for PAN-OS and Panorama.

QUESTION 9
What are three components of Cloud NGFW for AWS? (Choose three.)

A. Cloud NGFW Resource
B. Local or Global Rulestacks
C. Cloud NGFW Inspector
D. Amazon S3 bucket
E. Cloud NGFW Tenant

Correct Answer: A, B, C
Section:
Explanation:
Cloud NGFW for AWS is a Next-Generation Firewall as a Service. Its key components work together to provide comprehensive network security.
A . Cloud NGFW Resource: This represents the actual deployed firewall instance within your AWS environment. It's the core processing engine that inspects and secures network traffic. The Cloud NGFW resource is deployed in a VPC and associated with subnets, enabling traffic inspection between VPCs, subnets, and to/from the internet.
B . Local or Global Rulestacks: These define the security policies that govern traffic inspection. Rulestacks contain rules that match traffic based on various criteria (e.g., source/destination IP, port, application) and specify the action to take (e.g., allow, deny, inspect). Local Rulestacks are specific to a single Cloud NGFW resource, while Global Rulestacks can be shared across multiple Cloud NGFW resources for consistent policy enforcement.
C . Cloud NGFW Inspector: The Cloud NGFW Inspector is the core component performing the deep packet inspection and applying security policies. It resides within the Cloud NGFW Resource and analyzes network traffic based on the configured rulestacks. It provides advanced threat prevention capabilities, including intrusion prevention (IPS), malware detection, and URL filtering.
D . Amazon S3 bucket: While S3 buckets can be used for logging and storing configuration backups in some firewall deployments, they are not a core component of the Cloud NGFW architecture itself. Cloud NGFW uses its own logging and management infrastructure.
E . Cloud NGFW Tenant: The term 'Tenant' is usually associated with multi-tenant architectures where resources are shared among multiple customers. While Palo Alto Networks provides a managed service for Cloud NGFW, the deployment within your AWS account is dedicated and not considered a tenant in the traditional multi-tenant sense. The management of the firewall is done through Panorama or Cloud Management.
While direct, concise documentation specifically listing these three components in this exact format is difficult to pinpoint in a single document, the Palo Alto Networks documentation consistently describes these elements as integral. The concepts are spread across multiple documents and are best understood in context of the overall Cloud NGFW architecture:
Cloud NGFW for AWS Administration Guide: This is the primary resource for understanding Cloud NGFW. It details deployment, configuration, and management, covering the roles of the Cloud NGFW resource, rulestacks, and the underlying inspection engine. You can find this documentation on the Palo Alto Networks support portal by searching for 'Cloud NGFW for AWS Administration Guide'.

QUESTION 10
Which three methods may be used to deploy CN-Series firewalls? (Choose three.)

A. Terraform templates
B. Panorama plugin for Kubernetes
C. YAML file
D. Helm charts
E. Docker Swarm

Correct Answer: A, C, D
Section:
Explanation:
The CN-Series firewalls are containerized firewalls designed to protect Kubernetes environments. They offer several deployment methods to integrate with Kubernetes orchestration.
A . Terraform templates: Terraform is an Infrastructure-as-Code (IaC) tool that allows you to define and provision infrastructure using declarative configuration files. 1 Palo Alto Networks provides Terraform modules and examples to deploy CN-Series firewalls, enabling automated and repeatable deployments.
https://prathmeshh.hashnode.dev/day-62-terraform-and-docker
1. prathmeshh.hashnode.dev
https://prathmeshh.hashnode.dev/day-62-terraform-and-docker
prathmeshh.hashnode.dev
B . Panorama plugin for Kubernetes: While Panorama is used to manage CN-Series firewalls centrally, there isn't a direct 'Panorama plugin for Kubernetes' for deploying the firewalls themselves. Panorama is used for management after they're deployed using other methods.
C . YAML file: Kubernetes uses YAML files (manifests) to define the desired state of deployments, including pods, services, and other resources. You can deploy CN-Series firewalls by creating YAML files that define the necessary Kubernetes objects, such as Deployments, Services, and ConfigMaps. This is a core method for Kubernetes deployments.
D . Helm charts: Helm is a package manager for Kubernetes. Helm charts package Kubernetes resources, including YAML files, into reusable and shareable units. Palo Alto Networks provides Helm charts for deploying CN-Series firewalls, simplifying the deployment process and managing updates.
E . Docker Swarm: Docker Swarm is a container orchestration tool, but CN-Series firewalls are specifically designed for Kubernetes and are not deployed using Docker Swarm.
The Palo Alto Networks documentation clearly outlines these deployment methods:
CN-Series Deployment Guide: This is the primary resource for deploying CN-Series firewalls. It provides detailed instructions and examples for using Terraform, YAML files, and Helm charts. You can find this on the Palo Alto Networks support portal by searching for 'CN-Series Deployment Guide'.

QUESTION 11
What are two benefits of using a Palo Alto Networks NGFW in a public cloud environment? (Choose two.)

A. Complete security solution for the public cloud provider's physical host regardless of security measures
B. Automatic scaling of NGFWs to meet the security needs of growing applications and public cloud environments
C. Ability to manage the public cloud provider's physical hosts
D. Consistent Security policy to inbound, outbound, and east-west network traffic throughout the multi-cloud environment

Correct Answer: B, D
Section:
Explanation:
Using a Palo Alto Networks Next-Generation Firewall (NGFW) in a public cloud environment offers several key advantages related to security and scalability:
A . Complete security solution for the public cloud provider's physical host regardless of security measures: Palo Alto Networks NGFWs operate at the network layer (and above), inspecting traffic flowing in and out of your virtual networks (VPCs in AWS, VNETs in Azure, etc.). They do not provide security for the underlying physical infrastructure of the cloud provider. That's the cloud provider's responsibility. NGFWs secure your workloads within the cloud environment.
B . Automatic scaling of NGFWs to meet the security needs of growing applications and public cloud environments: This is a significant benefit. Cloud NGFWs can often be configured to auto-scale based on traffic demands. As your applications grow and require more bandwidth and processing, the NGFW can automatically scale up its resources (or deploy additional instances) to maintain performance and security. This elasticity is a core advantage of cloud-based firewalls.
C . Ability to manage the public cloud provider's physical hosts: As mentioned above, NGFWs do not provide management capabilities for the cloud provider's physical infrastructure. You manage your virtual network resources and the NGFW itself, but not the underlying hardware.
D . Consistent Security policy to inbound, outbound, and east-west network traffic throughout the multi-cloud environment: This is a crucial advantage, especially in multi-cloud deployments. Palo Alto Networks NGFWs allow

you to enforce consistent security policies across different cloud environments (AWS, Azure, GCP, etc.). This ensures consistent protection regardless of where your workloads are running and simplifies security management. East-west traffic (traffic between workloads within the same cloud environment) is also a key focus, as it's often overlooked by traditional perimeter-based security.

QUESTION 12
Which two software firewall types can protect egress traffic from workloads attached to an Azure vWAN hub? (Choose two.)

A. Cloud NGFW
B. PA-Series
C. CN-Series
D. VM-Series

Correct Answer: A, D
Section:
Explanation:
Azure vWAN (Virtual WAN) is a networking service that connects on-premises locations, branches, and Azure virtual networks. Protecting egress traffic from workloads attached to a vWAN hub requires a solution that can integrate with the vWAN architecture.
A . Cloud NGFW: Cloud NGFW is designed for cloud environments and integrates directly with Azure networking services, including vWAN. It can be deployed as a secured virtual hub or as a spoke VNet insertion to protect egress traffic.
B . PA-Series: PA-Series are hardware appliances and are not directly deployable within Azure vWAN. They would require complex configurations involving on-premises connectivity and backhauling traffic, which is not a typical or recommended vWAN design.
C . CN-Series: CN-Series is designed for containerized environments and is not suitable for protecting general egress traffic from workloads connected to a vWAN hub.
D . VM-Series: VM-Series firewalls can be deployed in Azure virtual networks that are connected to the vWAN hub. They can then be configured to inspect and control egress traffic. This is a common deployment model for VM-Series in Azure.

QUESTION 13
What can a firewall use to automatically update Security policies with new IP address information for a virtual machine (VM) when it has moved from host-A to host-B because host-A is down or undergoing periodic maintenance?

A. Dynamic Address Groups
B. Dynamic User Groups
C. Dynamic Host Groups
D. Dynamic IP Groups

Correct Answer: A
Section:
Explanation:
When a virtual machine moves between hosts and its IP address changes (or if it's assigned a new IP from a pool), traditional static security policies become ineffective. Dynamic Address Groups solve this problem.
A . Dynamic Address Groups: These groups automatically update their membership based on criteria such as tags, VM names, or other dynamic attributes. When a VM moves and its IP address changes, the Dynamic Address Group automatically updates its membership, ensuring that security policies remain effective without manual intervention. This is the correct solution for this scenario.
B . Dynamic User Groups: These groups are based on user identity and are used for user-based policy enforcement, not for tracking IP addresses of VMs.
C . Dynamic Host Groups: This is not a standard Palo Alto Networks term.
D . Dynamic IP Groups: While the concept sounds similar, the official Palo Alto Networks terminology is 'Dynamic Address Groups.' They achieve the functionality described in the question.

QUESTION 14
Which two public cloud service provider (CSP) environments offer, through their marketplace, a Cloud NGFW under the CSP's own brand name? (Choose two.)

A. Oracle Cloud Infrastructure (OCI)
B. IBM Cloud (previously Softlayer)

C. Alibaba Cloud
D. Google Cloud Platform (GCP)

Correct Answer: A, D
Section:
Explanation:
The question asks about Cloud NGFW offerings under the CSP's own brand name. This means the CSP is offering the service as their own, even though it's powered by Palo Alto Networks technology.
A . Oracle Cloud Infrastructure (OCI): OCI offers Oracle Cloud Infrastructure Network Firewall, which is powered by Palo Alto Networks' Cloud NGFW technology. It is branded as an Oracle service.
B . IBM Cloud (previously Softlayer): While Palo Alto Networks products can be deployed in IBM Cloud, there isn't a branded Cloud NGFW offering by IBM itself.
C . Alibaba Cloud: Similar to IBM Cloud, while Palo Alto Networks products can be used, Alibaba Cloud does not offer a rebranded Cloud NGFW service.
D . Google Cloud Platform (GCP): GCP offers Network Firewall Plus, which is powered by Palo Alto Networks' Cloud NGFW technology. It is branded as a Google

QUESTION 15
Which three tools are available to customers to facilitate the simplified and/or best-practice configuration of Palo Alto Networks Next-Generation Firewalls (NGFWs)? (Choose three.)

A. Telemetry to ensure that Palo Alto Networks has full visibility into the firewall configuration
B. Day 1 Configuration through the customer support portal (CSP)
C. Policy Optimizer to help identify and recommend Layer 7 policy changes
D. Expedition to enable the creation of custom threat signatures
E. Best Practice Assessment (BPA) in Strata Cloud Manager (SCM)

Correct Answer: C, D, E
Section:
Explanation:
Palo Alto Networks provides several tools to simplify NGFW configuration and ensure best practices are followed:
A . Telemetry to ensure that Palo Alto Networks has full visibility into the firewall configuration: While telemetry is crucial for monitoring and threat intelligence, it doesn't directly facilitate configuration in a simplified or best-practice manner. Telemetry provides data about the configuration and its performance, but it doesn't guide the configuration process itself.
B . Day 1 Configuration through the customer support portal (CSP): The CSP offers resources and documentation, but it doesn't provide a specific 'Day 1 Configuration' tool that automates or simplifies initial setup in a guided way. The initial configuration is typically done through the firewall's web interface or CLI.
C . Policy Optimizer to help identify and recommend Layer 7 policy changes: This is a key tool for simplifying and optimizing security policies. Policy Optimizer analyzes traffic logs and provides recommendations for refining Layer 7 policies based on application usage. This helps reduce policy complexity and improve security posture by ensuring policies are as specific as possible.
D . Expedition to enable the creation of custom threat signatures: Expedition is a migration tool that can also be used to create custom App-IDs and threat signatures. While primarily for migrations, its ability to create custom signatures helps tailor the firewall's protection to specific environments and applications, which is a form of configuration optimization.
E . Best Practice Assessment (BPA) in Strata Cloud Manager (SCM): The BPA is a powerful tool that analyzes firewall configurations against Palo Alto Networks best practices. It provides detailed reports with recommendations for improving security, performance, and compliance. This is a direct way to ensure configurations adhere to best practices.
Palo Alto Networks documentation highlights these tools:
Policy Optimizer documentation: Search for 'Policy Optimizer' on the Palo Alto Networks support portal. This documentation explains how the tool analyzes traffic and provides policy recommendations.
Expedition documentation: Search for 'Expedition' on the Palo Alto Networks support portal. This documentation describes its migration and custom signature creation capabilities.
Strata Cloud Manager documentation: Search for 'Strata Cloud Manager' or 'Best Practice Assessment' within the SCM documentation on the support portal. This will provide details on how the BPA works and the types of recommendations it provides.
These references confirm that Policy Optimizer, Expedition (for custom signatures), and the BPA in SCM are tools specifically designed to facilitate simplified and best-practice configuration of Palo Alto Networks NGFWs.

QUESTION 16
Which two statements accurately describe cloud-native load balancing with Palo Alto Networks VM-Series firewalls and/or Cloud NGFW in public cloud environments? (Choose two.)

A. Cloud NGFW's distributed architecture model requires deployment of a single centralized firewall and will force all traffic to the firewall across pre-built VPN tunnels.
B. VM-Series firewall deployments in the public cloud will require the deployment of a cloud-native load balancer if high availability (HA) or redundancy is needed.
C. Cloud NGFW in AWS or Azure has load balancing built into the underlying solution and does not require the deployment of a separate load balancer.

D. VM-Series firewall load balancing is automated and is handled by the internal mechanics of the NGFW software without the need for a load balancer.

Correct Answer: B, C
Section:
Explanation:
Cloud-native load balancing with Palo Alto Networks firewalls in public clouds involves understanding the distinct approaches for VM-Series and Cloud NGFW:
A . Cloud NGFW's distributed architecture model requires deployment of a single centralized firewall and will force all traffic to the firewall across pre-built VPN tunnels: This is incorrect. Cloud NGFW uses a distributed architecture where traffic is steered to the nearest Cloud NGFW instance, often using Gateway Load Balancers (GWLBs) or similar services. It does not rely on a single centralized firewall or force all traffic through VPN tunnels.
B . VM-Series firewall deployments in the public cloud will require the deployment of a cloud-native load balancer if high availability (HA) or redundancy is needed: This is correct. VM-Series firewalls, when deployed for HA or redundancy, require a cloud-native load balancer (e.g., AWS ALB/NLB/GWLB, Azure Load Balancer) to distribute traffic across the active firewall instances. This ensures that if one firewall fails, traffic is automatically directed to a healthy instance.
C . Cloud NGFW in AWS or Azure has load balancing built into the underlying solution and does not require the deployment of a separate load balancer: This is also correct. Cloud NGFW integrates with cloud-native load balancing services (e.g., Gateway Load Balancer in AWS) as part of its architecture. This provides automatic scaling and high availability without requiring you to manage a separate load balancer.
D . VM-Series firewall load balancing is automated and is handled by the internal mechanics of the NGFW software without the need for a load balancer: This is incorrect. VM-Series firewalls do not have built-in load balancing capabilities for HA. A cloud-native load balancer is essential for distributing traffic and ensuring redundancy.
Cloud NGFW documentation: Look for sections on architecture, traffic steering, and integration with cloud-native load balancing services (like AWS Gateway Load Balancer).
VM-Series deployment guides for each cloud provider: These guides explain how to deploy VM-Series firewalls for HA using cloud-native load balancers.
These resources confirm that VM-Series requires external load balancers for HA, while Cloud NGFW has load balancing integrated into its design.

QUESTION 17
What three benefits does flex licensing for VM-Series firewalls offer? (Choose three.)

A. Licensing additional memory resources to increase session capacity
B. Licensing Strata Cloud Manager, Panorama with Dedicated Log Collectors, and CDSS per deployment profile
C. Using a pool of credits for both CN-Series firewall and VM-Series firewall deployment profiles
D. Moving credits between public and private cloud VM-Series firewall deployments
E. Vertically scaling the number of licensed cores in an existing fixed deployment profile

Correct Answer: C, D, E
Section:
Explanation:
Flex licensing provides flexibility in how you consume Palo Alto Networks firewall capabilities, especially in cloud environments:
A . Licensing additional memory resources to increase session capacity: Flex licensing primarily focuses on CPU cores and does not directly license memory resources. Memory is tied to the instance size you select in the cloud provider.
B . Licensing Strata Cloud Manager, Panorama with Dedicated Log Collectors, and CDSS per deployment profile: Strata Cloud Manager, Panorama, and CDSS are licensed separately and are not part of the flex licensing model for VM-Series.
C . Using a pool of credits for both CN-Series firewall and VM-Series firewall deployment profiles: This is a key benefit of flex licensing. You can use a shared pool of credits to deploy both CN-Series (containerized) and VM-Series (virtual machine) firewalls, providing flexibility in your deployment strategy.
D . Moving credits between public and private cloud VM-Series firewall deployments: This is another significant advantage. Flex licensing allows you to transfer credits between public cloud (AWS, Azure, GCP) and private cloud VM-Series deployments, optimizing resource utilization and cost.
E . Vertically scaling the number of licensed cores in an existing fixed deployment profile: Flex licensing allows you to dynamically adjust the number of licensed cores for your VM-Series firewalls. This vertical scaling enables you to meet changing performance demands without needing to redeploy or reconfigure your firewalls significantly.
Palo Alto Networks Flex Licensing documentation: Search for 'Flex Licensing' on the Palo Alto Networks support portal. This documentation provides detailed information about the flex licensing model, including the benefits and use cases.
This documentation confirms that sharing credits between CN-Series and VM-Series, moving credits between public and private clouds, and vertically scaling licensed cores are core benefits of flex licensing.

QUESTION 18
A partner has successfully showcased and validated the efficacy of the Palo Alto Networks software firewall to a customer.
Which two additional partner-delivered or Palo Alto Networks-delivered common options can the sales team offer to the customer before the sale is completed? (Choose two.)

A. Hardware collection and recycling services by Palo Alto Networks or by an approved NextWave Partner for the customer's existing firewall infrastructure
B. Professional services delivered by Palo Alto Networks or by an approved Certified Professional Services Partner (CPSP) for deployment assistance or QuickStart
C. Network encryption services (NES) delivered by an approved NES partner to ensure none of the data traversed is readable by third-party entities
D. Managed services delivered by an approved Managed Security Services Program (MSSP) partner for day-to-day management of the environment

Correct Answer: B, D
Section:
Explanation:
After a successful software firewall demonstration, the sales team can offer additional services to facilitate the customer's adoption and ongoing management:
A . Hardware collection and recycling services by Palo Alto Networks or by an approved NextWave Partner for the customer's existing firewall infrastructure: While some partners might offer recycling services independently, this isn't a standard offering directly tied to the Palo Alto Networks sales process before a sale is completed. Recycling or trade-in programs are often handled separately or after a purchase.
B . Professional services delivered by Palo Alto Networks or by an approved Certified Professional Services Partner (CPSP) for deployment assistance or QuickStart: This is a common and valuable offering. Professional services can help customers with initial deployment, configuration, and knowledge transfer, ensuring a smooth transition and maximizing the value of the firewall. QuickStart packages are a specific type of professional service designed for rapid deployment.
C . Network encryption services (NES) delivered by an approved NES partner to ensure none of the data traversed is readable by third-party entities: While encryption is a crucial aspect of security, offering separate NES services from a specific 'NES partner' isn't a standard pre-sales offering related to firewall deployment. The NGFW itself provides various encryption capabilities (e.g., VPNs, SSL decryption).
D . Managed services delivered by an approved Managed Security Services Program (MSSP) partner for day-to-day management of the environment: Offering managed services is a common pre-sales option. MSSPs can handle ongoing monitoring, management, and maintenance of the firewall, allowing the customer to focus on their core business.
Information about these services can be found on the Palo Alto Networks website and partner portal:
Partner programs: Information about CPSPs and MSSPs can be found in the Palo Alto Networks partner program documentation.
Professional services: Details about Palo Alto Networks professional services offerings, including QuickStart packages, are available on their website.
These resources confirm that professional services (including QuickStart) and managed services are standard pre-sales options.

QUESTION 19
Which three resources can help conduct planning and implementation of Palo Alto Networks NGFW solutions? (Choose three.)

A. Technical assistance center (TAC)
B. Partners / systems Integrators
C. Professional services
D. Proof of Concept Labs
E. QuickStart services

Correct Answer: B, C, E
Section:
Explanation:
Several resources are available to assist with planning and implementing Palo Alto Networks NGFW solutions:
A . Technical assistance center (TAC): While TAC provides support for existing deployments, they are generally not directly involved in the initial planning and implementation phases. TAC helps with troubleshooting and resolving issues after the firewall is deployed.
B . Partners / systems Integrators: Partners and system integrators play a crucial role in planning and implementation. They possess expertise in network design, security best practices, and Palo Alto Networks products, enabling them to design and deploy solutions tailored to customer needs.
C . Professional services: Palo Alto Networks professional services offer expert assistance with all phases of the project, from planning and design to implementation and knowledge transfer. They can provide specialized skills and best-practice guidance.
D . Proof of Concept Labs: While valuable for testing and validating solutions, Proof of Concept (POC) labs are more focused on evaluating the technology before a full-scale implementation. They are not the primary resources for the actual planning and implementation process itself, though they can inform it.
E . QuickStart services: QuickStart packages are a type of professional service specifically designed for rapid deployment. They provide a structured approach to implementation, accelerating the time to value.
Information about these resources can be found on the Palo Alto Networks website and partner portal:
Partner locator: The Palo Alto Networks website has a partner locator tool to find certified partners and system integrators.

Professional services: Details about Palo Alto Networks professional services offerings, including QuickStart packages, are available on their website.
These resources confirm that partners/system integrators, professional services (including QuickStart), are key resources for planning and implementation. While TAC and POCs have roles, they are not the primary resources for this phase.

QUESTION 20
A company wants to make its flexible-license VM-Series firewall, which runs on ESXi, process higher throughput. Which order of steps should be followed to minimize downtime?

A. Increase the vCPU within the deployment profile. Retrieve or fetch license keys on the VM-Series NGFW. Power-off the VM and increase the vCPUs within the hypervisor. Power-on the VM-Series NGFW. Confirm the correct tier level and vCPU appear on the NGFW dashboard.
B. Power-off the VM and increase the vCPUs within the hypervisor. Power-on the VM-Series NGFW. Retrieve or fetch license keys on the VM-Series NGFW. Increase the vCPU within the deployment profile. Confirm the correct tier level and vCPU appear on the NGFW dashboard.
C. Power-off the VM and increase the vCPUs within the hypervisor. Increase the vCPU within the deployment profile. Retrieve or fetch license keys on the VM-Series NGFW. Confirm the correct tier level and vCPU appear on the NGFW dashboard. Power-on the VM-Series NGFW.
D. Increase the vCPU within the deployment profile. Retrieve or fetch license keys on the VM-Series NGFW. Confirm the correct tier level and vCPU appear on the NGFW dashboard. Power-off the VM and increase the vCPUs within the hypervisor. Power-on the VM-Series NGFW.

Correct Answer: A
Section:
Explanation:
To minimize downtime when increasing throughput on a flexible-license VM-Series firewall running on ESXi, the following steps should be taken:
Increase the vCPU within the deployment profile: This is the first step. By increasing the vCPU allocation in the licensing profile, you prepare the license system for the change. This does not require a VM reboot.
Retrieve or fetch license keys on the VM-Series NGFW: After adjusting the licensing profile, the firewall needs to retrieve the updated license information to reflect the new vCPU allocation. This can be done via the web UI or CLI and usually does not require a reboot.
Power-off the VM and increase the vCPUs within the hypervisor: Now that the license is prepared, the VM can be powered off, and the vCPUs can be increased within the ESXi hypervisor settings.
Power-on the VM-Series NGFW: After increasing the vCPUs in the hypervisor, power on the VM. The firewall will now use the allocated resources and the updated license.
Confirm the correct tier level and vCPU appear on the NGFW dashboard: Finally, verify in the firewall's web UI or CLI that the correct license tier and vCPU count are reflected.
This order minimizes downtime because the licensing changes are handled before the VM is rebooted.
While not explicitly documented in a single, numbered step list, the concepts are covered in the VM-Series deployment guides and licensing documentation:
VM-Series Deployment Guides: These guides explain how to configure vCPUs and licensing.
Flex Licensing Documentation: This explains how license allocation works with vCPUs.
These resources confirm that adjusting the license profile before the VM reboot is crucial for minimizing downtime.

QUESTION 21
A Cloud NGFW for Azure can be deployed to which two environments? (Choose two.)

A. Azure Kubernetes Service (AKS)
B. Azure Virtual WAN
C. Azure DevOps
D. Azure VNET

Correct Answer: B, D
Section:
Explanation:
Cloud NGFW for Azure is designed to secure network traffic within and between Azure environments:
A . Azure Kubernetes Service (AKS): While CN-Series firewalls are designed for securing Kubernetes environments like AKS, Cloud NGFW is not directly deployed within AKS. Instead, Cloud NGFW secures traffic flowing to and from AKS clusters.
B . Azure Virtual WAN: Cloud NGFW can be deployed to secure traffic flowing through Azure Virtual WAN hubs. This allows for centralized security inspection of traffic between on-premises networks, branch offices, and Azure virtual networks.
C . Azure DevOps: Azure DevOps is a set of development tools and services. Cloud NGFW is a network security solution and is not directly related to Azure DevOps.

D . Azure VNET: Cloud NGFW can be deployed to secure traffic within and between Azure Virtual Networks (VNETs). This is its primary use case, providing advanced threat prevention and network security for Azure workloads.
The Cloud NGFW for Azure documentation clearly describes these deployment scenarios:
Cloud NGFW for Azure Documentation: Search for 'Cloud NGFW for Azure' on the Palo Alto Networks support portal. This documentation explains how to deploy Cloud NGFW in VNETs and integrate it with Virtual WAN.
This confirms that Azure VNETs and Azure Virtual WAN are the supported deployment environments for Cloud NGFW.

QUESTION 22
Which three statements describe benefits of Palo Alto Networks Cloud-Delivered Security Services (CDSS) over other vendor solutions? (Choose three.)

A. Individually targeted products provide better security than platform solutions.
B. Multi-vendor best-of-breed products provide security coverage on a per-use-case basis.
C. It requires no additional performance overhead when enabling additional features.
D. It provides simplified management through fewer consoles for more effective security coverage.
E. It significantly reduces the total cost of ownership for the customer.

Correct Answer: C, D, E
Section:
Explanation:
Palo Alto Networks Cloud-Delivered Security Services (CDSS) offer several advantages over other security solutions:
A . Individually targeted products provide better security than platform solutions: This is generally the opposite of Palo Alto Networks' philosophy. CDSS is a platform approach, integrating multiple security functions into a unified service. This integrated approach is often more effective than managing disparate point solutions.
B . Multi-vendor best-of-breed products provide security coverage on a per-use-case basis: While 'best-of-breed' has its merits, managing multiple vendors increases complexity and can lead to integration challenges. CDSS provides a comprehensive set of security services from a single vendor, simplifying management and integration.
C . It requires no additional performance overhead when enabling additional features: This is a key advantage of CDSS. Because the services are cloud-delivered and integrated into the platform, enabling additional security functions typically does not introduce significant performance overhead on the firewall itself.
D . It provides simplified management through fewer consoles for more effective security coverage: CDSS is managed through Panorama or Strata Cloud Manager, providing a single pane of glass for managing multiple security functions. This simplifies management compared to managing separate consoles for different security products.
E . It significantly reduces the total cost of ownership for the customer: By consolidating security functions into a single platform and reducing management overhead, CDSS can help reduce the total cost of ownership compared to deploying and managing separate point solutions.
Information about CDSS and its benefits can be found on the Palo Alto Networks website and in their marketing materials:
CDSS overview: Search for 'Cloud-Delivered Security Services' on the Palo Alto Networks website. This will provide information on the benefits and features of CDSS.
These resources highlight the advantages of CDSS in terms of performance, simplified management, and reduced TCO.

QUESTION 23
What are three valid methods that use firewall flex credits to activate VM-Series firewall licenses by specifying authcode? (Choose three.)

A. /config/bootstrap.xml file of complete bootstrapping package
B. /license/authcodes file of complete bootstrap package
C. Panorama device group in Panorama SW Licensing Plugin
D. authcodes= key value pair of Azure Vault configuration
E. authcodes= key value pair of basic bootstrapping configuration

Correct Answer: A, B, E
Section:
Explanation:
Firewall flex credits and authcodes are used to license VM-Series firewalls. The methods for using authcodes during bootstrapping include:
A . /config/bootstrap.xml file of complete bootstrapping package: The bootstrap.xml file is a key component of the bootstrapping process. It can contain the authcode for licensing.
B . /license/authcodes file of complete bootstrap package: A dedicated authcodes file within the bootstrap package is another valid method for providing license information.
C . Panorama device group in Panorama SW Licensing Plugin: While Panorama manages licenses, specifying authcodes directly via a device group is not the typical method for bootstrapping. Panorama usually manages

licenses after the firewalls are bootstrapped and connected to Panorama.
D . authcodes= key value pair of Azure Vault configuration: While using Azure Key Vault for storing and retrieving secrets (like authcodes) is a good security practice for ongoing operations, it's not the primary method for initial bootstrapping using flex credits. Bootstrapping typically relies on the local bootstrap package.
E . authcodes= key value pair of basic bootstrapping configuration: This refers to including the authcode directly in the bootstrapping configuration, such as in the init-cfg.txt file or via cloud-init.

QUESTION 24
A company has used software NGFW credits to deploy several VM-Series firewalls with Advanced URL Filtering in the company's deployment profiles. The IT department has determined that the firewalls no longer need the Advanced URL Filtering license.
How can this license be removed from the hosts?

A. Edit the current deployment profile to remove the Advanced URL Filtering license.
B. On the firewall, issue this command: > delete url subscription license.
C. Add a new deployment profile with all the licenses selected except Advanced URL Filtering.
D. Delete the current deployment profile from the cloud service provider.

Correct Answer: A
Section:
Explanation:
Software NGFW credits and deployment profiles manage licenses for VM-Series firewalls.
A . Edit the current deployment profile to remove the Advanced URL Filtering license: This is the correct approach. Deployment profiles are used to define the licenses associated with VM-Series firewalls. Modifying the profile directly updates the licensing for all firewalls using that profile.
B . On the firewall, issue this command: > delete url subscription license: This command does not exist. Licenses are managed through the deployment profile, not directly on the firewall via CLI in this context.
C . Add a new deployment profile with all the licenses selected except Advanced URL Filtering: While this would work, it's less efficient than simply editing the existing profile.
D . Delete the current deployment profile from the cloud service provider: This is too drastic. Deleting the profile would remove all licensing and configuration associated with it, not just the Advanced URL Filtering license.