



Palo Alto Networks PSE-SFW-Pro-24 Practice Questions

Shared by Cooke on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

Which two products can be deployed using Terraform for automation and integration? (Choose two.)

Options:

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

Answer:

B, C

Explanation:

Comprehensive and Detailed In-Depth Step-by-Step Explanation:

Terraform is an Infrastructure-as-Code (IaC) tool that automates the provisioning and configuration of infrastructure, including Palo Alto Networks firewalls. The Palo Alto Networks Systems Engineer Professional - Software Firewall documentation specifies which firewall products support Terraform integration for deployment and automation in cloud and virtualized environments.

VM-Series firewall (Option B): Terraform can be used to deploy VM-Series firewalls in public clouds (e.g., AWS, Azure, GCP), private clouds, or on-premises virtualized environments. Palo Alto Networks provides Terraform modules and scripts (available on GitHub) to automate VM-Series deployment, configuration, and integration with cloud-native services, ensuring scalability and repeatability. The documentation highlights Terraform as a key automation tool for VM-Series, aligning with DevOps practices.

CN-Series firewall (Option C): CN-Series firewalls, designed for containerized environments, can be deployed using Terraform in conjunction with Kubernetes. Terraform scripts automate the provisioning of infrastructure (e.g., Kubernetes clusters in AWS, Azure, or GCP) and integrate with CN-Series for securing container workloads. The documentation notes Terraform's role in automating CN-Series deployments, leveraging Kubernetes manifests and cloud-native integrations.

Options A (PA-Series firewall) and D (Cloud NGFW) are incorrect. PA-Series firewalls are physical appliances, not virtual or software-based, and do not support Terraform deployment, as Terraform focuses on cloud and virtualized infrastructure, not hardware. Cloud NGFW is a cloud-native managed service in AWS and Azure, and while it can be managed or deployed

through automation, it does not use Terraform directly for deployment, as it relies on cloud provider APIs and native scaling mechanisms, not IaC tools like Terraform.

Question 2

Question Type: MultipleChoice

What are two benefits of credit-based flexible licensing for software firewalls? (Choose two.)

Options:

- A- Create virtual Panoramas.
- B- Add Cloud-Delivered Security Services (CDSS) subscriptions to CN-Series firewalls.
- C- Create Cloud NGFWs.
- D- Add Cloud-Delivered Security Services (CDSS) subscriptions to PA-Series firewalls.

Answer:

B, C

Explanation:

Credit-based flexible licensing provides flexibility in deploying and managing Palo Alto Networks software firewalls. Let's analyze the options:

- A . Create virtual Panoramas: While Panorama can manage software firewalls, credit-based licensing is primarily focused on the firewalls themselves (VM-Series, CN-Series, Cloud NGFW), not on Panorama. Panorama has its own licensing model.
- B . Add Cloud-Delivered Security Services (CDSS) subscriptions to CN-Series firewalls: This is a VALID benefit. Credit-based licensing allows customers to use credits to enable CDSS subscriptions (like Threat Prevention, URL Filtering, WildFire) on CN-Series firewalls. This provides flexibility in choosing and applying security services as needed.
- C . Create Cloud NGFWs: This is a VALID benefit. Cloud NGFW for AWS and Azure are licensed through a credit-based system. Customers consume credits based on usage.
- D . Add Cloud-Delivered Security Services (CDSS) subscriptions to PA-Series firewalls: PA-Series firewalls are hardware appliances and use traditional licensing methods. Credit-based licensing is not applicable to them.

Question 3

Question Type: MultipleChoice

Which statement correctly describes behavior when using Ansible to automate configuration changes on a PAN-OS firewall or in Panorama?

Options:

- A- Ansible can only be used to automate configuration changes on physical firewalls but not virtual firewalls.
- B- Ansible requires direct access to the firewall's CLI to make changes.
- C- Ansible uses the XML API to make configuration changes to PAN-OS.
- D- Ansible requires the use of Python to create playbooks.

Answer:

C

Explanation:

Ansible interacts with PAN-OS through its API.

Why C is correct: Ansible uses the PAN-OS XML API to manage configurations. This allows for programmatic interaction and automation.

Why A, B, and D are incorrect:

A . Ansible can only be used to automate configuration changes on physical firewalls but not virtual firewalls: Ansible can manage both physical (PA-Series) and virtual (VM-Series, CN-Series) firewalls.

B . Ansible requires direct access to the firewall's CLI to make changes: Ansible does not require direct CLI access. It uses the API, which is more structured and secure.

D . Ansible requires the use of Python to create playbooks: While Ansible playbooks are written in YAML, you don't need to write Python code directly. Ansible modules handle the underlying API interactions. The pan-os-python SDK is a separate tool that can be used for more complex automation tasks, but it's not required for basic Ansible playbooks.

Palo Alto Networks Reference:

Ansible Collections for Palo Alto Networks: These collections, available on Ansible Galaxy, provide modules for interacting with PAN-OS via the API.

Palo Alto Networks Documentation on API Integration: The API documentation describes how to use the XML API for configuration management.

Palo Alto Networks GitHub Repositories: Palo Alto Networks provides examples and resources on using Ansible with PAN-OS.

Question 4

Question Type: MultipleChoice

A prospective customer plans to migrate multiple applications to Amazon Web Services (AWS) and is considering deploying Palo Alto Networks NGFWs to protect these workloads from threats. The customer currently uses Panorama to manage on-premises firewalls and wants to avoid additional management complexity.

Which AWS deployment option meets the customer's technical and business value requirements while minimizing risk exposure?

Options:

- A- Software NGFW credits and Strata Cloud Manager (SCM)
- B- Cloud NGFWs and Panorama
- C- Cloud NGFWs and Strata Cloud Manager (SCM)
- D- Software NGFW credits and Panorama

Answer:

B

Explanation:

Comprehensive and Detailed In-Depth Step-by-Step Explanation:

The customer's requirements involve securing AWS workloads with Palo Alto Networks NGFWs, maintaining consistency with their existing Panorama management for on-premises firewalls, and minimizing management complexity and risk exposure. The Palo Alto Networks Systems Engineer Professional - Software Firewall documentation provides guidance on deploying NGFWs in AWS, focusing on compatibility with existing management tools.

Cloud NGFWs and Panorama (Option B): Cloud NGFW for AWS is a cloud-native firewall service that integrates with Panorama for centralized management, ensuring consistency with the customer's existing on-premises firewall management. Panorama provides unified policy enforcement, logging, and monitoring for both on-premises firewalls and Cloud NGFW instances in AWS, avoiding additional management complexity. The documentation highlights this as the ideal solution for customers leveraging Panorama, minimizing risk by maintaining a single management platform while providing advanced threat prevention and application visibility for

AWS workloads.

Options A (Software NGFW credits and Strata Cloud Manager [SCM]), C (Cloud NGFWs and Strata Cloud Manager [SCM]), and D (Software NGFW credits and Panorama) are incorrect. SCM (Options A, C) is a cloud-delivered management solution but does not integrate as seamlessly with on-premises firewalls managed by Panorama, introducing complexity for the customer. Software NGFW credits (Options A, D) alone do not specify a deployment option; they are a licensing model, not a firewall type, and do not address management needs directly. Option D omits the specific firewall type (Cloud NGFW) needed for AWS, making it incomplete for meeting the customer's requirements.

Question 5

Question Type: MultipleChoice

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

Options:

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

Answer:

A, B, C

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 6

Question Type: MultipleChoice

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.)

Options:

- 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.

Answer:

B, C

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 7

Question Type: MultipleChoice

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?

Options:

- 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.

Answer:

A

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 8

Question Type: MultipleChoice

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

Options:

- 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.

Answer:

C, D, E

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.



To Get Premium Files for PSE-SFW-Pro-24
Visit

<https://www.p2pexams.com/products/pse-swfw-pro-24>

For More Free Questions Visit

<https://www.p2pexams.com/palo-alto-networks/pdf/pse-swfw-pro-24>

