Palo Alto Networks

NGFW-ENGINEER Exam

Palo Alto Networks Next-Generation Firewall Engineer

Questions & Answers
Demo

Version: 4.0

Question: 1

To maintain security efficacy of its public cloud resources by using native tools, a company purchases Cloud NGFW credits to replicate the Panorama, PA-Series, and VM-Series devices used in physical data centers. Resources exist on AWS and Azure:
The AWS deployment is architected with AWS Transit Gateway, to which all resources connect
The Azure deployment is architected with each application independently routing traffic
The engineer deploying Cloud NGFW in these two cloud environments must account for the following:
Minimize changes to the two cloud environments
Scale to the demands of the applications while using the least amount of compute resources
Allow the company to unify the Security policies across all protected areas
Which two implementations will meet these requirements? (Choose two.)

A. Deploy a VM-Series firewall in AWS in each VPC, create an IPSec tunnel between AWS and Azure, and manage the policy with Panorama.
B. Deploy Cloud NGFW for Azure in vNET/s, update the vNET/s routing to path traffic through the deployed NGFWs, and manage the policy with Panorama.
C. Deploy Cloud NGFW for Azure in vWAN, create a vWAN to route all appropriate traffic to the Cloud NGFW attached to the vWAN, and manage the policy with local rules.
D. Deploy Cloud NGFW for AWS in a centralized Security VPC, update the Transit Gateway to route all appropriate traffic through the Security VPC, and manage the policy with Panorama.

Answer: B, D

Explanation:
To meet the company's requirements - minimizing changes to the cloud environments, optimizing compute resources, and unifying security policies - the best approach is to deploy Cloud NGFW solutions natively for AWS and Azure while managing policies centrally with Panorama.
In Azure, using Cloud NGFW for Azure deployed within vNETs allows traffic to be routed through security appliances efficiently without requiring a complete re-architecture. This approach aligns with Azure's existing routing mechanism while maintaining security.
In AWS, deploying Cloud NGFW for AWS in a centralized Security VPC and integrating it with AWS Transit Gateway enables traffic inspection for all connected VPCs without modifying individual workloads. This method ensures efficient scaling and minimal infrastructure changes while maintaining security consistency.

Question: 2

During an upgrade to the routing infrastructure in a customer environment, the network

administrator wants to implement Advanced Routing Engine (ARE) on a Palo Alto Networks firewall. Which firewall models support this configuration?

A. PA-5280, PA-7080, PA-3250, VM-Series
B. PA-455, VM-Series, PA-1410, PA-5450
C. PA-3260, PA-5410, PA-850, PA-460
D. PA-7050, PA-1420, VM-Series, CN-Series

Answer: C

Explanation:
The Advanced Routing Engine (ARE) is supported on Palo Alto Networks firewalls that utilize the PAN-OS 11.0+ software and have the required hardware architecture. The supported models include PA-3200 Series, PA-5400 Series, PA-800 Series, and PA-400 Series. These models provide enhanced routing capabilities, including BGP, OSPF, and more complex routing policies.
PA-3260 and PA-5410 are part of the PA-3200 and PA-5400 Series, which are known to support ARE.
PA-850 and PA-460 are within the PA-800 and PA-400 Series, which also support ARE

Question: 3

Which two statements apply to configuring required security rules when setting up an IPSec tunnel between a Palo Alto Networks firewall and a third- party gateway? (Choose two.)

A. For incoming and outgoing traffic through the tunnel, creating separate rules for each direction is optional.
B. The IKE negotiation and IPSec/ESP packets are allowed by default via the intrazone default allow policy.
C. For incoming and outgoing traffic through the tunnel, separate rules must be created for each direction.
D. The IKE negotiation and IPSec/ESP packets are denied by default via the interzone default deny policy.

Answer: C, D

Explanation:
Separate rules must be created for each direction: Palo Alto Networks firewalls enforce security policies based on traffic direction. To allow bidirectional communication through the IPSec tunnel, two separate rules are required - one for incoming and one for outgoing traffic.

IKE negotiation and IPSec/ESP packets are denied by default: Palo Alto Networks firewalls use an interzone default deny policy, meaning that unless an explicit policy allows IKE (UDP 500/4500) and ESP (protocol 50) traffic, the firewall will block these packets, preventing tunnel establishment. Therefore, administrators must create explicit rules permitting IKE and IPSec/ESP traffic to the firewall's external interface.

Question: 4

Which statement describes the role of Terraform in deploying Palo Alto Networks NGFWs?

A. It acts as a logging service for NGFW performance metrics.
B. It orchestrates real-time traffic inspection for network segments.
C. It provides Infrastructure-as-Code (IaC) to automate NGFW deployment.
D. It manages threat intelligence data synchronization with NGFWs.

Answer: C

Explanation:
Terraform is an Infrastructure-as-Code (IaC) tool that automates the provisioning and management of infrastructure resources, including Palo Alto Networks Next-Generation Firewalls (NGFWs). By using Terraform configuration files, administrators can define and deploy NGFW instances across cloud environments (such as AWS, Azure, and GCP) efficiently and consistently.
Terraform enables:
Automated firewall deployment in cloud environments.
Configuration of security policies and networking settings in a declarative manner.
Scalability and repeatability, reducing manual intervention in firewall provisioning.

Question: 5

By default, which type of traffic is configured by service route configuration to use the management interface?

A. Security zone
B. IPSec tunnel
C. Virtual system (VSYS)
D. Autonomous Digital Experience Manager (ADEM)

Answer: D

Explanation:
By default, the Autonomous Digital Experience Manager (ADEM) traffic is configured to use the management interface in a Palo Alto Networks firewall. The management interface is typically used for management-related traffic, such as monitoring and logging, and it is configured to handle ADEM-related traffic for the optimal performance of digital experience monitoring features.
This default configuration helps ensure that ADEM traffic does not interfere with regular traffic that may traverse other interfaces, such as traffic from security zones or IPSec tunnels.