# Free Questions for PCSFE by vceexamstest

## Shared by Beard on 05-09-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

**Question Type:** **MultipleChoice**

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

## Options:

**A-** Device

**B-** Notify

**C-** Address

**D-** Template

## Answer:

C

## Explanation:

Address groups are the type of groups that allow sharing cloud-learned tags with on-premises firewalls. Address groups are dynamic objects that can include IP addresses or tags as members. Cloud-learned tags are tags that are assigned to cloud resources by cloud providers or third-party tools. By using address groups with cloud-learned tags, you can apply consistent security policies across your hybrid cloud environment. Reference: [Address Groups]

# Question 2

**Question Type: MultipleChoice**

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

## Options:

**A-** It protects data center and internet gateway deployments.

**B-** It allows for automatic deployment, provisioning, and immediate policy enforcement without any manual intervention.

**C-** It ensures consistent security across the entire environment.

**D-** It allows extension of Zero Trust Network Security to the most remote locations and smallest branches.

## Answer:

B

### Explanation:

A benefit of CN-Series firewalls securing traffic between pods and other workload types is that it allows for automatic deployment, provisioning, and immediate policy enforcement without any manual intervention. CN-Series firewalls are integrated with Kubernetes and use the Kubernetes API server to get information about pod labels, namespaces, services, and network policies. CN-Series firewalls can also use Panorama or Terraform to automate the configuration and management of security policies. Reference: [CN-Series Deployment Guide]

## Question 3

**Question Type: MultipleChoice**

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

### Options:

**A-** Assignment of identical licenses and subscriptions

**B-** Deployment on a different host

**C-** Configuration of asymmetric routing

**D-** Deployment on same type of hypervisor

### Answer:

A, B

### Explanation:

To deploy VM-Series firewalls in high availability (HA), you need to assign identical licenses and subscriptions, and deploy them on a different host. Assigning identical licenses and subscriptions ensures that both firewalls have the same features and capabilities. Deploying them on a different host ensures that they are not affected by the same host failure. Reference: [VM-Series High Availability]

# Question 4

**Question Type: MultipleChoice**

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.)

### Options:

**A-** Transit VPC and Security VPC

**B-** Traditional active-active HA

**C-** Transit gateway and Security VPC

**D-** Traditional active-passive HA

## Answer:

C, D

## Explanation:

Palo Alto Networks recommends two configuration options for outbound high availability (HA) design in Amazon Web Services using a VM-Series firewall: transit gateway and Security VPC, and traditional active-passive HA. Transit gateway and Security VPC allows you to use a single transit gateway to route traffic between multiple VPCs and the internet, while using a Security VPC to host the VM-Series firewalls. Traditional active-passive HA allows you to use two VM-Series firewalls in an HA pair, where one firewall is active and handles all traffic, while the other firewall is passive and takes over in case of a failure. Reference: [VM-Series Deployment Guide for AWS Outbound VPC]

# Question 5

**Question Type: MultipleChoice**

Which service, when enabled, provides inbound traffic protection?

## Options:

**A-** Advanced URL Filtering (AURLF)

**B-** Threat Prevention

**C-** Data loss prevention (DLP)

**D-** DNS Security

## Answer:

D

## Explanation:

DNS Security is a service that provides inbound traffic protection by preventing DNS-based attacks. DNS Security uses machine learning and threat intelligence to identify and block malicious domains, command and control (C2) traffic, and DNS tunneling.

Reference: [DNS Security]

# Question 6

**Question Type: MultipleChoice**

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

## Options:

**A-** Aperture orchestration engine

**B-** Client-ID

**C-** Dynamic Address Groups

**D-** API Key

## Answer:

D

## Explanation:

To integrate a Palo Alto Networks VM-Series firewall with Azure Orchestration, you need an API Key. The API Key is used to authenticate and authorize requests from Azure Orchestration to the VM-Series firewall. The API Key is generated on the VM-Series firewall and copied to Azure Orchestration. Reference: [Azure Orchestration Integration with Palo Alto Networks VM-Series Firewalls]

# Question 7

**Question Type:** **MultipleChoice**

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

## Options:

**A-** SDN code hooks can help detonate malicious file samples designed to detect virtual environments.

**B-** Traffic can be automatically redirected using static address objects.

**C-** Service graphs are configured to allow their deployment.

**D-** VXLAN or NVGRE traffic is terminated and inspected for translation to VLANs.

## Answer:

C

## Explanation:

Palo Alto Networks Next-Generation Firewalls (NGFWs) are deployed within a Cisco ACI architecture using service graphs. Service graphs are logical representations of how traffic flows through different network services, such as firewalls, load balancers, or routers. By configuring service graphs, you can insert NGFWs into the traffic path and apply security policies to the traffic. Reference: [Palo Alto Networks NGFW Integration with Cisco ACI]

# Question 8

**Question Type: MultipleChoice**

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

## Options:

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

**B-** Obtain the Amazon Machine Images (AMIs) from marketplace.

**C-** Enable communication between Panorama and the NSX Manager.

**D-** Register the VM-Series firewall as a service.

## Answer:

C, D

### Explanation:

To deploy a VM-Series firewall on NSX, you need to enable communication between Panorama and the NSX Manager. This allows Panorama to receive information about the virtual machines and services in the NSX environment. You also need to register the VM-Series firewall as a service on the NSX Manager.This allows NSX to redirect traffic to the VM-Series firewall for inspection3.

Reference:VM-Series Deployment Guide for VMware NSX

## Question 9

**Question Type: MultipleChoice**

Why are containers uniquely suitable for runtime security based on allow lists?

### Options:

**A-** Containers have only a few defined processes that should ever be executed.

**B-** Developers define the processes used in containers within the Dockerfile.

**C-** Docker has a built-in runtime analysis capability to aid in allow listing.

**D-** Operations teams know which processes are used within a container.

## Answer:

A

## Explanation:

Containers are uniquely suitable for runtime security based on allow lists because containers have only a few defined processes that should ever be executed. Developers can specify the processes that are allowed to run in a container using a Dockerfile, but this does not guarantee that only those processes will run at runtime.Therefore, using an allow list approach can prevent any unauthorized or malicious processes from running in a container2. Reference:Container Security