PCSFE Q&As

Palo Alto Networks Certified Software Firewall Engineer (PCSFE)

Pass Palo Alto Networks PCSFE Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/pcsfe.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

A. They are located outside the cluster and have no visibility into application-level cluster traffic.

B. They do not scale independently of the Kubernetes cluster.

C. They are managed by another entity when located inside the cluster.

D. They function differently based on whether they are located inside or outside of the cluster.

Correct Answer: A

Explanation: VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster are problematic for protecting containerized workloads because they are located outside the cluster and have no visibility into application-level cluster traffic. Kubernetes is a platform that provides orchestration, automation, and management of containerized applications. Kubernetes cluster traffic consists of traffic between containers within a pod, across pods, or across namespaces. VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster cannot inspect or control this traffic, as they only see the encapsulated or aggregated traffic at the network layer. This creates blind spots and security gaps for containerized workloads. VM-Series firewalls and hardware firewalls that are external to the Kubernetes cluster are not problematic for protecting containerized workloads because they do not scale independently of the Kubernetes cluster, are managed by another entity when located inside the cluster, or function differently based on whether they are located inside or outside of the cluster, as those are not valid reasons or scenarios for firewall deployment in a Kubernetes environment. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [CN-Series Concepts], [VM-Series on Kubernetes]

QUESTION 2

What is a design consideration for a prospect who wants to deploy VM-Series firewalls in an Amazon Web Services (AWS) environment?

A. Special AWS plugins are needed for load balancing.

B. Resources are shared within the cluster.

C. Only active-passive high availability (HA) is supported.

D. High availability (HA) clusters are limited to fewer than 8 virtual appliances.

Correct Answer: C

Explanation: A design consideration for a prospect who wants to deploy VM-Series firewalls in an Amazon Web Services (AWS) environment is that only active-passive high availability (HA) is supported. High availability (HA) is a feature that provides redundancy and failover protection for firewalls in case of hardware or software failure. Active-passive HA is a mode of HA that consists of two firewalls in a pair, where one firewall is active and handles all traffic, while the other firewall is passive and acts as a backup. Active-passive HA is the only mode of HA that is supported for VM-Series firewalls in an AWS environment, due to the limitations of AWS networking and routing. Active-active HA, which is another mode of HA that consists of two firewalls in a pair that both handle traffic and synchronize sessions, is not supported for VM-Series firewalls in an AWS environment. A design consideration for a prospect who wants to deploy VM-Series firewalls in an AWS environment is not that special AWS plugins are needed for load balancing, resources are shared within the cluster, or high availability (HA) clusters are limited to fewer than 8 virtual appliances, as

those are not valid or relevant factors for firewall deployment in an AWS environment. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [High Availability Overview], [High Availability on AWS]

QUESTION 3

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

A. VRLAN

B. Geneve

C. GRE

D. VMLAN

Correct Answer: B

Explanation: Geneve is the protocol used for communicating between VM-Series firewalls and a gateway load balancer in Amazon Web Services (AWS). A gateway load balancer is a type of network load balancer that distributes traffic across multiple virtual appliances, such as VM-Series firewalls, in AWS. Geneve is a tunneling protocol that encapsulates the original packet with an additional header that contains metadata about the source and destination endpoints, as well as other information. Geneve allows the gateway load balancer to preserve the original packet attributes and forward it to the appropriate VM- Series firewall for inspection and processing. VRLAN, GRE, and VMLAN are not protocols used for communicating between VM-Series firewalls and a gateway load balancer in AWS, but they are related concepts that can be used for other purposes. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploy the VM-Series Firewall with AWS Gateway Load Balancer], [Geneve Protocol Specification]

QUESTION 4

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 Network > Interfaces.

C. Select the Config tab. then select New Route from the Security Zone Route drop-down menu.

D. Select Network > Virtual Router, then select the default link to open the Virtual Router dialog.

Correct Answer: AD

Explanation: To configure a default route to an internet router, you need to select Network > Virtual Router, then select the default link to open the Virtual Router dialog. Then, select the Static Routes tab, then click Add. You can then specify the destination as 0.0.0.0/0 and the next hop as the IP address of the internet router1. References: Palo Alto Networks Certified Software Firewall Engineer (PCSFE)

QUESTION 5

What are two requirements for automating service deployment of a VM-Series firewall from an NSX Manager? (Choose two.)

A. vCenter has been given Palo Alto Networks subscription licenses for VM-Series firewalls.

B. Panorama has been configured to recognize both the NSX Manager and vCenter.

C. The deployed VM-Series firewall can establish communications with Panorama.

D. Panorama can establish communications to the public Palo Alto Networks update servers.

Correct Answer: BC

Explanation: The two requirements for automating service deployment of a VM-Series firewall from an NSX Manager are: Panorama has been configured to recognize both the NSX Manager and vCenter. The deployed VM-Series firewall can establish communications with Panorama. NSX Manager is a software component that provides centralized management and control of the NSX environment, including network virtualization, automation, and security. Service deployment is a process that involves deploying and configuring network services, such as firewalls, load balancers, or routers, on the NSX environment. VM-Series firewall is a virtualized version of the Palo Alto Networks next-generation firewall that can be deployed on various cloud or virtualization platforms, including NSX. Panorama is a centralized management server that provides visibility and control over multiple Palo Alto Networks firewalls and devices. Panorama has been configured to recognize both the NSX Manager and vCenter is a requirement for automating service deployment of a VM-Series firewall from an NSX Manager. vCenter is a software component that provides centralized management and control of the VMware environment, including hypervisors, virtual machines, and other resources. Panorama has been configured to recognize both the NSX Manager and vCenter by adding them as VMware service managers and enabling service insertion for VM-Series firewalls on NSX. This allows Panorama to communicate with the NSX Manager and vCenter, retrieve information about the NSX environment, and deploy and manage VM-Series firewalls as network services on the NSX environment. The deployed VM-Series firewall can establish communications with Panorama is a requirement for automating service deployment of a VM-Series firewall from an NSX Manager. The deployed VM-Series firewall can establish communications with Panorama by registering with Panorama using its serial number or IP address, and receiving configuration updates and policy rules from Panorama. This allows the VM-Series firewall to operate as part of the Panorama management domain, synchronize its settings and status with Panorama, and report its logs and statistics to Panorama. vCenter has been given Palo Alto Networks subscription licenses for VM-Series firewalls and Panorama can establish communications to the public Palo Alto Networks update servers are not requirements for automating service deployment of a VM-Series firewall from an NSX Manager, as those are not related or relevant factors for service deployment automation. References: [Palo Alto Networks Certified Software Firewall Engineer (PCSFE)], [Deploy the VM-Series Firewall on VMware NSX-T], [Panorama Overview], [VMware Service Manager], [Register the Firewall with Panorama]