Free Questions for PCSFE by go4braindumps

Shared by Allen on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which PAN-OS feature allows for automated updates to address objects when VM-Series firewalls are setup as part of an NSX deployment?

Options:

A- Boundary automation

B- Hypervisor integration

C- Bootstrapping

D- Dynamic Address Group

Answer:

D

Explanation:

Dynamic Address Group is the PAN-OS feature that allows for automated updates to address objects when VM-Series firewalls are setup as part of an NSX deployment. NSX is a software-defined network (SDN) solution that provides network virtualization, automation, and security for cloud-native applications. Dynamic Address Group is an object that represents a group of IP addresses based on criteria such as tags, regions, interfaces, or user-defined attributes. Dynamic Address Group allows Security policies to adapt dynamically to changes in the network topology or workload characteristics without requiring manual updates. When VM-Series firewalls are setup as part of an NSX deployment, they can leverage the NSX tags assigned to virtual machines (VMs) or containers by the NSX manager or controller to populate Dynamic Address Groups and update Security policies accordingly. Boundary automation, Hypervisor integration, and Bootstrapping are not PAN-OS features that allow for automated updates to address objects when VM-Series firewalls are setup as part of an NSX deployment, but they are related concepts that can be used for other purposes. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Dynamic Address Groups Overview], [Deploy the VM-Series Firewall on VMware NSX]

Question 2

Question Type: MultipleChoice

Which component allows the flexibility to add network resources but does not require making changes to existing policies and rules?

Options:

A- Content-ID

B- External dynamic list

C- App-ID

D- Dynamic address group

Answer:

D

Explanation:

Dynamic address group is the component that allows the flexibility to add network resources but does not require making changes to existing policies and rules. Dynamic address group is an object that represents a group of IP addresses based on criteria such as tags, regions, interfaces, or user-defined attributes. Dynamic address group allows Security policies to adapt dynamically to changes in the network topology or workload characteristics without requiring manual updates. Content-ID, External dynamic list, and App-ID are not components that allow the flexibility to add network resources but do not require making changes to existing policies and rules, but they are related features that can enhance security and visibility. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Dynamic Address Groups Overview], [Content-ID Overview], [External Dynamic Lists Overview], [App-ID Overview]

Question 3

Question Type: **MultipleChoice**

How must a Palo Alto Networks Next-Generation Firewall (NGFW) be configured in order to secure traffic in a Cisco ACI environment?

Options:

A- It must be deployed as a member of a device cluster

B- It must use a Layer 3 underlay network

C- It must receive all forwarding lookups from the network controller

D- It must be identified as a default gateway

Answer:

B

Explanation:

A Palo Alto Networks Next-Generation Firewall (NGFW) must be configured to use a Layer 3 underlay network in order to secure traffic in a Cisco ACI environment. A Layer 3 underlay network is a physical network that provides IP connectivity between devices, such as routers, switches, and firewalls. A Palo Alto Networks NGFW must use a Layer 3 underlay network to communicate with the Cisco ACI fabric and receive traffic redirection from the Cisco ACI policy-based redirect mechanism. A Palo Alto Networks NGFW does not need to be deployed as a member of a device cluster, receive all forwarding lookups from the network controller, or be identified as a default gateway in order to secure traffic in a Cisco ACI environment, as those are not valid requirements or options for firewall integration with Cisco ACI. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploy the VM-Series Firewall on Cisco ACI], [Cisco ACI Underlay Network]

Question 4

Question Type: **MultipleChoice**

A customer in a VMware ESXi environment wants to add a VM-Series firewall and partition an existing group of virtual machines (VMs) in the same subnet into two groups. One group requires no additional security, but the second group requires substantially more security.

How can this partition be accomplished without editing the IP addresses or the default gateways of any of the guest VMs?

Options:

A- Edit the IP address of all of the affected VMs. www*

B- Create a new virtual switch and use the VM-Series firewall to separate virtual switches using virtual wire mode. Then move the guests that require more security into the new virtual switch.

C- Create a Layer 3 interface in the same subnet as the VMs and then configure proxy Address Resolution Protocol (ARP).

D- Send the VLAN out of the virtual environment into a hardware Palo Alto Networks firewall in Layer 3 mode. Use the same IP address as the old default gateway, then delete it.

Answer:

B

Explanation:

The partition can be accomplished without editing the IP addresses or the default gateways of any of the guest VMs by creating a new virtual switch and using the VM-Series firewall to separate virtual switches using virtual wire mode. Then move the guests that require more security into the new virtual switch. A virtual switch is a software-based switch that connects virtual machines (VMs) in a VMware ESXi environment. A virtual wire is a deployment mode of the VM-Series firewall that allows it to act as a bump in the wire between two network segments, without requiring an IP address or routing configuration. By creating a new virtual switch and using the VM-Series firewall to separate virtual switches using virtual wire mode, the customer can isolate the group of VMs that require more security from the rest of the network, and apply security policies to the traffic passing through the firewall. The partition cannot be accomplished without editing the IP addresses or the default gateways of any of the guest VMs by editing the IP address of all of the affected VMs, creating a Layer 3 interface in the same subnet as the VMs and then configuring proxy Address Resolution Protocol (ARP), or sending the VLAN out of the virtual environment into a hardware Palo Alto Networks firewall in Layer 3 mode. Use the same IP address as the old default gateway, then delete it, as those methods would require changing the network configuration of the guest VMs or introducing additional complexity and latency. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploying Virtual Switches], [Virtual Wire Deployment], [Deploying Virtual Wire on VMware ESXi]

Question 5

Question Type: MultipleChoice

Which two deployment modes of VM-Series firewalls are supported across NSX-T? (Choose two.)

Options:

A- Prism Central

B- Bootstrap

C- Service Cluster

D- Host-based

Answer:

B, C

Explanation:

The two deployment modes of VM-Series firewalls that are supported across NSX-T are:

Bootstrap

Service Cluster

NSX-T is a software-defined network (SDN) solution that provides network virtualization, automation, and security for cloud-native applications. Bootstrap is a method of deploying and configuring VM-Series firewalls in NSX-T using a bootstrap package that contains the initial setup information, such as licenses, certificates, software updates, and configuration files. Service Cluster is a mode of deploying VM-Series firewalls in NSX-T as a group of firewalls that act as a single logical firewall to provide scalability and high availability. Prism Central, Host-based, and Service Insertion are not deployment modes of VM-Series firewalls in NSX-T, but they are related concepts that can be used for other purposes. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploy the VM-Series Firewall on NSX-T], [Bootstrap the VM-Series Firewall for NSX-T], [Deploy the VM-Series Firewall as a Service Cluster on NSX-T]

Question 6

Question Type: MultipleChoice

Which component scans for threats in allowed traffic?

Options:

A- Intelligent Traffic Offload

B- TLS decryption

C- Security profiles

D- NAT

Answer:

C

Explanation:

Security profiles are the components that scan for threats in allowed traffic. Security profiles are sets of rules or settings that define how the firewall will inspect and handle traffic based on various threat prevention technologies, such as antivirus, anti-spyware, vulnerability protection, URL filtering, file blocking, data filtering, and WildFire analysis. Security profiles can be applied to Security policy rules to enforce granular protection against known and unknown threats in allowed traffic. Intelligent Traffic Offload, TLS decryption, and NAT are not components that scan for threats in allowed traffic, but they are related features that can enhance security and performance.

Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Security Profiles Overview], [Threat Prevention Datasheet]

Question 7

Question Type: **MultipleChoice**

Which two elements of the Palo Alto Networks platform architecture enable security orchestration in a software-defined network (SDN)? (Choose two.)

Options:

A- Full set of APIs enabling programmatic control of policy and configuration

B- VXLAN support for network-layer abstraction

C- Dynamic Address Groups to adapt Security policies dynamically

D- NVGRE support for advanced VLAN integration

Answer:

A, C

Explanation:

The two elements of the Palo Alto Networks platform architecture that enable security orchestration in a software-defined network (SDN) are:

Full set of APIs enabling programmatic control of policy and configuration

Dynamic Address Groups to adapt Security policies dynamically

The Palo Alto Networks platform architecture consists of four key elements: natively integrated security technologies, full set of APIs, cloud-delivered services, and centralized management. The full set of APIs enables programmatic control of policy and configuration across the platform, allowing for automation and integration with SDN controllers and orchestration tools. Dynamic Address Groups are objects that represent groups of IP addresses based on criteria such as tags, regions, interfaces, or user-defined attributes. Dynamic Address Groups allow Security policies to adapt dynamically to changes in the network topology or workload characteristics without requiring manual updates. VXLAN support for network-layer abstraction and NVGRE support for advanced VLAN integration are not elements of the Palo Alto Networks platform architecture, but they are features that support SDN deployments. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Palo Alto Networks Platform Architecture], [API Overview], [Dynamic Address Groups Overview]

Question 8

Question Type: **MultipleChoice**

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

Options:

A- VRLAN

B- Geneve

C- GRE

D- VMLAN

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. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploy the VM-Series Firewall with AWS Gateway Load Balancer], [Geneve Protocol Specification]

Question 9

Question Type: **MultipleChoice**

How is traffic directed to a Palo Alto Networks firewall integrated with Cisco ACI?

Options:

A- By using contracts between endpoint groups that send traffic to the firewall using a shared policy

B- Through a virtual machine (VM) monitor domain

C- Through a policy-based redirect

D- By creating an access policy

Answer:

C

Explanation:

Traffic is directed to a Palo Alto Networks firewall integrated with Cisco ACI through a policy-based redirect. Cisco ACI is a software-defined network (SDN) solution that provides network automation, orchestration, and visibility. A policy-based redirect is a mechanism that allows Cisco ACI to redirect traffic from one endpoint group (EPG) to another EPG through a service device, such as a Palo Alto Networks firewall. The firewall can then inspect and enforce security policies on the redirected traffic before sending it back to Cisco ACI. Traffic is not directed to a Palo Alto Networks firewall integrated with Cisco ACI by using contracts between endpoint groups that send traffic to the firewall using a shared policy, through a virtual machine (VM) monitor domain, or by creating an access policy, as those are not valid methods for traffic redirection in Cisco ACI. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [Deploy the VM-Series Firewall on Cisco ACI], [Cisco ACI Policy-Based Redirect]

Question 10

Question Type: **MultipleChoice**

What can software next-generation firewall (NGFW) credits be used to provision?

Options:

A- Remote browser isolation

B- Virtual Panorama appliances

C- Migrating NGFWs from hardware to VMs

D- Enablement of DNS security

Answer:

C

Explanation:

Software next-generation firewall (NGFW) credits can be used to provision migrating NGFWs from hardware to VMs. Software NGFW credits are a flexible licensing model that allows customers to purchase and consume software NGFWs as needed, without having to specify the platform or deployment model upfront. Customers can use software NGFW credits to migrate their existing hardware NGFWs to VM-Series firewalls on any supported cloud or virtualization platform, or to deploy new VM-Series firewalls as their needs grow. Software NGFW credits cannot be used to provision remote browser isolation, virtual Panorama appliances, or enablement of DNS security, as those are separate solutions that require different licenses or subscriptions. Reference:Palo Alto Networks Certified Software

Firewall Engineer (PCSFE), [Software NGFW Credits Datasheet], [Software NGFW Credits FAQ]

Question 11

Question Type: **MultipleChoice**

Which two statements apply to the VM-Series plugin? (Choose two.)

Options:

A- It can manage capabilities common to both VM-Series firewalls and hardware firewalls.

B- It can be upgraded independently of PAN-OS.

C- It enables management of cloud-specific interactions between VM-Series firewalls and supported public cloud platforms.

D- It can manage Panorama plugins.

Answer:

B, C

Explanation:

The two statements that apply to the VM-Series plugin are:

It can be upgraded independently of PAN-OS.

It enables management of cloud-specific interactions between VM-Series firewalls and supported public cloud platforms.

The VM-Series plugin is a software component that extends the functionality of the PAN-OS operating system to support cloud-specific features and APIs. The VM-Series plugin can be upgraded independently of PAN-OS to provide faster access to new cloud capabilities and integrations. The VM-Series plugin enables management of cloud-specific interactions between VM-Series firewalls and supported public cloud platforms, such as AWS, Azure, GCP, Alibaba Cloud, and Oracle Cloud. These interactions include bootstrapping, licensing, scaling, high availability, load balancing, and tagging. The VM-Series plugin cannot manage capabilities common to both VM-Series firewalls and hardware firewalls, as those are handled by PAN-OS. The VM-Series plugin cannot manage Panorama plugins, as those are separate software components that extend the functionality of the Panorama management server to support cloud-specific features and APIs. Reference:Palo Alto Networks Certified Software Firewall Engineer (PCSFE), [VM-Series Plugin Overview], [VM-Series Plugin Release Notes]