Free Questions for PSE-SoftwareFirewall by certsdeals

Shared by Wood on 18-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

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 (EDL)

C- Dynamic address group

D- App-ID

Answer:

C

Explanation:

Dynamic address groups in Palo Alto Networks firewalls provide flexibility by allowing network resources to be added without requiring changes to existing policies and rules:

Dynamic address group: These groups automatically update based on tags and attributes assigned to network objects. When new resources are added with the appropriate tags, they are dynamically included in the address group, and the associated policies automatically apply to them without manual intervention.

Question 2

Question Type: MultipleChoice

Which two factors lead to improved return on investment for prospects interested in Palo Alto Networks virtualized next-generation firewalls (NGFWs)? (Choose two.)

Options:

A- Reduced operational expenditures

B- Decreased likelihood of data breach

C- Reduced insurance premiums

D- Reduced time to deploy

Answer:

A, D

Explanation:

Prospects interested in Palo Alto Networks virtualized next-generation firewalls (NGFWs) can achieve improved return on investment (ROI) through the following factors:

Reduced operational expenditures: Virtualized NGFWs reduce the need for physical hardware, lowering the costs associated with purchasing, maintaining, and managing hardware appliances. This also includes savings on power, cooling, and physical space requirements.

Reduced time to deploy: Virtual NGFWs can be quickly deployed in various environments, such as public clouds or virtualized data centers, compared to the time-consuming process of installing physical hardware. This agility allows organizations to respond faster to security needs and market demands.

Question 3

Question Type: MultipleChoice

Which feature provides real-time analysis using machine learning (ML) to defend against new and unknown threats?

Options:

A- Cortex Data Lake

B- DNS Security

C- Panorama VM-Series plugin

D- Advanced URL Filtering (AURLF)

Answer:

D

Explanation:

Advanced URL Filtering (AURLF) leverages machine learning (ML) to provide real-time analysis and defense against new and unknown threats:

Real-time analysis: AURLF uses ML models to analyze web traffic in real-time, identifying malicious URLs and preventing access to harmful content before it reaches the user.

Defending against new and unknown threats: The ML capabilities allow the system to detect and block previously unknown threats by analyzing patterns and behaviors associated with malicious URLs, ensuring a proactive security posture.

Question 4

Question Type: MultipleChoice

What must be enabled when using Terraform templates with a Cloud next-generation firewall (NGFW) for Amazon Web Services (AWS)?

Options:

A- Access to the Cloud NGFW for AWS console

B- AWS Firewall Manager console access

C- AWS CloudWatch logging

D- Access to the Palo Alto Networks Customer Support Portal

Answer:

A

Explanation:

When using Terraform templates with a Cloud next-generation firewall (NGFW) for Amazon Web Services (AWS), you must enable access to the Cloud NGFW for AWS console to manage and deploy firewall resources effectively:

Access to the Cloud NGFW for AWS console: This access is crucial for the initial setup, configuration, and ongoing management of the Cloud NGFW resources. Terraform templates automate the provisioning and management of these resources, but initial access to the console is necessary to configure and retrieve necessary information (such as API keys and configuration details) for the Terraform scripts.

Question 5

Question Type: MultipleChoice

What can be implemented in a CN-Series to protect communications between Dockers?

Options:

A- Data loss prevention (DLP)

B- Firewalling

C- Runtime security

D- Vulnerability management

Answer:

B

Explanation:

In a CN-Series (Cloud Native) environment, protecting communications between Docker containers is crucial. CN-Series firewalls are designed to provide advanced firewalling capabilities within containerized environments:

Firewalling: The CN-Series firewall provides Layer 7 visibility, allowing for application-layer security policies and protections. It ensures that all inter-container traffic is inspected, filtered, and secured according to the defined security policies. This includes blocking malicious traffic, preventing unauthorized access, and providing micro-segmentation within the Kubernetes clusters.

Question 6

Question Type: MultipleChoice

Which two methods of Zero Trust implementation can benefit an organization? (Choose two.)

Options:

A- Boundaries are established.

B- Security automation is seamlessly integrated.

C- Compliance is validated.

D- Access controls are enforced.

Answer:

B, D

Explanation:

Zero Trust implementation revolves around the principle that no entity, inside or outside the network, should be trusted by default. The primary methods that benefit an organization are:

Security automation is seamlessly integrated: Zero Trust requires continuous monitoring and verification of every device and user attempting to access resources. Automation helps in efficiently managing these processes, ensuring that security policies are consistently enforced without human error. Automated tools can quickly detect anomalies, respond to threats, and update access controls dynamically.

Access controls are enforced: Zero Trust models implement strict access controls based on the principle of least privilege. This means users and devices are given the minimum levels of access -- or permissions -- necessary to perform their jobs. Enforcing access controls ensures that only authenticated and authorized entities can access specific resources.

Question 7

Question Type: MultipleChoice

Which two subscriptions should be recommended to a customer who is deploying VM-Series firewalls to a private data center but is concerned about protecting data-center resources from malware and lateral movement? (Choose two.)

Options:

A- Threat Prevention

B- SD-WAN

C- Intelligent Traffic Offload

D- WildFire

Answer:

A, D

Explanation:

For a customer deploying VM-Series firewalls in a private data center and concerned about protecting resources from malware and lateral movement, the following subscriptions are recommended:

Threat Prevention: This subscription provides comprehensive threat detection and prevention capabilities, including IPS, anti-virus, anti-spyware, and vulnerability protection.

WildFire: This advanced threat intelligence service analyzes suspicious files and identifies new malware, providing protection against zero-day exploits and threats.

Palo Alto Networks Threat Prevention: Threat Prevention

Palo Alto Networks WildFire: WildFire

Question 8

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- Dynamic Address Group

B- Hypervisor integration

C- Bootstrapping

D- Boundary automation

Answer:

A

Explanation:

Dynamic Address Groups in PAN-OS allow for automated updates to address objects when VM-Series firewalls are set up as part of an NSX deployment. These address groups can dynamically include members based on criteria such as tags, enabling automated and flexible security policies that adjust to changes in the virtual environment.

Palo Alto Networks Dynamic Address Groups: Dynamic Address Groups

NSX and VM-Series Integration: NSX Integration Guide

Question 9

Question Type: MultipleChoice

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

Options:

A- Through a policy-based redirect (PBR)

B- By creating an access policy

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

D- Through a virtual machine (VM) monitor domain

Answer:

C

Explanation:

In Cisco ACI, traffic is directed to a Palo Alto Networks firewall by creating contracts between endpoint groups (EPGs) that send traffic to the firewall. These contracts define the policy for communication between EPGs, ensuring that traffic is inspected and secured by the firewall before reaching its destination.

Cisco ACI and Palo Alto Networks Integration Guide: Contracts and Policies

Cisco ACI Fundamentals: ACI Contracts

Question 10

Question Type: MultipleChoice

What helps avoid split brain in active-passive high availability (HA) pair deployment?

Options:

A- Enabling preemption on both firewalls in the HA pair

B- Using a standard traffic interface as the HA2 backup

C- Using a standard traffic interface as the HA3 link

D- Using the management interface as the HA1 backup link

Answer:

D

Explanation:

To avoid split brain scenarios in an active-passive high availability (HA) pair deployment, the management interface can be used as the HA1 backup link. This ensures reliable communication between the HA pair and prevents both firewalls from assuming the active role simultaneously, which can happen if they lose connectivity with each other on the primary HA1 link.

Palo Alto Networks High Availability Guide: HA Configuration

Best Practices for HA Configuration: Avoiding Split Brain

Question 11

Question Type: **MultipleChoice**

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

Options:

A- Traffic can be automatically redirected using static address objects.

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

C- Service graphs are configured to allow their deployment.

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

Answer:

C

Explanation:

Within a Cisco ACI architecture, Palo Alto Networks Next-Generation Firewalls (NGFWs) are deployed using service graphs. Service graphs in Cisco ACI define the sequence of network services that traffic must pass through. By configuring service graphs, administrators can seamlessly integrate Palo Alto Networks firewalls into the fabric to inspect and secure traffic flows.

Palo Alto Networks and Cisco ACI Integration Guide: Service Graphs Integration

Cisco ACI Service Graph Documentation: Service Graphs

Question 12

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- Traditional active-active HA

B- Transit gateway and Security VPC

C- Traditional active-passive HA

D- Transit VPC and Security VPC

Answer:

B, D

Explanation:

Transit Gateway and Security VPC:

Using a transit gateway in conjunction with a Security VPC is a recommended design for outbound high availability (HA) in AWS. This configuration ensures that traffic can be routed efficiently and securely through the VM-Series firewalls deployed in the Security VPC.

Palo Alto Networks AWS Design Guide

Transit VPC and Security VPC:

Another recommended approach is to use a Transit VPC along with a Security VPC. The Transit VPC provides a centralized routing hub, while the Security VPC hosts the VM-Series firewalls to inspect and secure outbound traffic.

Palo Alto Networks AWS Transit VPC Guide