IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **PSE-SWFW-Pro-24**

Title : Palo Alto Networks Systems Engineer Professional - Software Firewall

Version : DEMO

1.Which three solutions does Strata Cloud Manager (SCM) support? (Choose three.)
A. Prisma Cloud
B. CN-Series firewalls
C. Prisma Access
D. PA-Series firewalls
E. VM-Series firewalls
Answer: B, D, E
Explanation:
Strata Cloud Manager (SCM) is designed to simplify the management and operations of Palo Alto Networks next-generation firewalls. It provides centralized management and visibility across various deployment models.
Based on official Palo Alto Networks documentation, SCM directly supports the following firewall platforms:
B. CN-Series firewalls: SCM is used to manage containerized firewalls deployed in Kubernetes environments. It facilitates tasks like policy management, upgrades, and monitoring for CN-Series firewalls. This is clearly documented in Palo Alto Networks' CN-Series documentation and SCM administration guides.
D. PA-Series firewalls: SCM provides comprehensive management capabilities for hardware-based PA-Series firewalls. This includes tasks like device onboarding, configuration management, software updates, and log analysis. This is a core function of SCM and is extensively covered in their official documentation.
E. VM-Series firewalls: SCM also supports VM-Series firewalls deployed in various public and private cloud environments. It offers similar management capabilities as for PA-Series, including configuration, policy enforcement, and lifecycle management. This is explicitly mentioned in Palo Alto Networks' VM-Series and SCM documentation.
Why other options are incorrect:
A. Prisma Cloud: Prisma Cloud is a separate cloud security platform that focuses on cloud workload protection, cloud security posture management (CSPM), and cloud infrastructure entitlement management (CIEM). While there might be integrations between Prisma Cloud and other Palo Alto Networks products, Prisma Cloud itself is not directly managed by Strata Cloud Manager. They are distinct platforms with different focuses.
C. Prisma Access: Prisma Access is a cloud-delivered security platform that provides secure access to applications and data for remote users and branch offices. Like Prisma Cloud, it's a separate product, and while it integrates with other Palo Alto Networks offerings, it is not managed by Strata Cloud Manager. It has its own dedicated management plane.

2.A company has created a custom application that collects URLs from various websites and then lists bad sites. They want to update a custom URL category on the firewall with the URLs collected.
Which tool can automate these updates?
A. Dynamic User Groups
B. SNMP SET
C. Dynamic Address Groups
D. XMLAPI
Answer: D

Explanation:
The scenario describes a need for programmatic and automated updating of a custom URL category on a Palo Alto Networks firewall. The XML API is specifically designed for this kind of task. It allows external systems and scripts to interact with the firewall's configuration and operational data.
Here's why the XML API is the appropriate solution and why the other options are not:
D. XML API: The XML API provides a well-defined interface for making changes to the firewall's configuration. This includes creating, modifying, and deleting URL categories and adding or removing URLs within those categories. A script can be written to retrieve the list of "bad sites" from the company's application and then use the XML API to push those URLs into the custom URL category on the firewall. This process can be automated on a schedule. This is the most efficient and recommended method for this type of integration.
Why other options are incorrect:
A. Dynamic User Groups: Dynamic User Groups are used to dynamically group users based on attributes like username, group membership, or device posture. They are not relevant for managing URL categories.
B. SNMP SET: SNMP (Simple Network Management Protocol) is primarily used for monitoring and retrieving operational data from network devices. While SNMP can be used to make some configuration changes, it is not well-suited for complex configuration updates like adding multiple URLs to a category. The XML API is the preferred method for configuration changes.
C. Dynamic Address Groups: Dynamic Address Groups are used to dynamically populate address groups based on criteria like tags, IP addresses, or FQDNs. They are intended for managing IP addresses and not URLs, so they are not applicable to this scenario. Palo Alto Networks
Reference: The primary reference for this is the Palo Alto Networks XML API documentation. Searching the Palo Alto Networks support site (live.paloaltonetworks.com) for "XML API" will provide access to the latest documentation. This documentation details the various API calls available, including those for managing URL categories.
Specifically, you would look for API calls related to:
Creating or modifying custom URL categories.
Adding or removing URLs from a URL category.
The XML API documentation provides examples and detailed information on how to construct the XML requests and interpret the responses. This is crucial for developing a script to automate the URL updates.

3.What are three benefits of Palo Alto Networks VM-Series firewalls as they relate to direct integration with third-party network virtualization solution providers? (Choose three.)
A. Integration with Cisco ACI allows insertion of a virtual firewall and enforcement of dynamic policies between endpoint groups without the need for manual policy adjustments.
B. Integration with a third-party network virtualization solution allows management and deployment of the entire virtual network and hosts directly from Panorama.
C. Integration with Nutanix AHV allows the firewall to be dynamically informed of changes in the environment and ensures policy is applied to virtual machines (VMs) as they join the network.
D. Integration with VMware NSX provides comprehensive visibility and security of all virtualized data center traffic including intra-host ESXi virtual machine (VM) communications.
E. Integration with network virtualization solution providers allows manual deployment and management

of firewall rules through multiple interfaces and front ends specific to each technology.
Answer: A, C, D
Explanation:
The question focuses on the benefits of VM-Series firewalls concerning direct integration with third-party network virtualization solutions.
A. Integration with Cisco ACI allows insertion of a virtual firewall and enforcement of dynamic policies between endpoint groups without the need for manual policy adjustments. This is a key benefit. The integration between Palo Alto Networks VM-Series and Cisco ACI automates the insertion of the firewall into the traffic path and enables dynamic policy enforcement based on ACI endpoint groups (EPGs). This eliminates manual policy adjustments and simplifies operations.
C. Integration with Nutanix AHV allows the firewall to be dynamically informed of changes in the environment and ensures policy is applied to virtual machines (VMs) as they join the network. This is also a core advantage. The integration with Nutanix AHV allows the VM-Series firewall to be aware of VM lifecycle events (creation, deletion, migration). This dynamic awareness ensures that security policies are automatically applied to VMs as they are provisioned or moved within the Nutanix environment.
D. Integration with VMware NSX provides comprehensive visibility and security of all virtualized data center traffic including intra-host ESXi virtual machine (VM) communications. This is a significant benefit. The integration between VM-Series and VMware NSX provides granular visibility and security for all virtualized traffic, including east-west (VM-to-VM) traffic within the same ESXi host.
This level of microsegmentation is crucial for securing modern data centers.
Why other options are incorrect:
B. Integration with a third-party network virtualization solution allows management and deployment of the entire virtual network and hosts directly from Panorama. While Panorama provides centralized management for VM-Series firewalls, it does not manage the underlying virtual network infrastructure or hosts of third-party providers like VMware NSX or Cisco ACI. These platforms have their own management planes. Panorama manages the security policies and firewalls, not the entire virtualized infrastructure.
E. Integration with network virtualization solution providers allows manual deployment and management of firewall rules through multiple interfaces and front ends specific to each technology. This is the opposite of what integration aims to achieve. The purpose of integration is to automate and simplify management, not to require manual configuration through multiple interfaces. Direct integration aims to reduce manual intervention and streamline operations. Palo Alto Networks
Reference: To verify these points, you can refer to the following types of documentation on the Palo Alto Networks support site (live.paloaltonetworks.com):
VM-Series Deployment Guides: These guides often have sections dedicated to integrations with specific virtualization platforms like VMware NSX, Cisco ACI, and Nutanix AHV.
Solution Briefs and White Papers: Palo Alto Networks publishes documents outlining the benefits and technical details of these integrations.
Technology Partner Pages: On the Palo Alto Networks website, there are often pages dedicated to technology partners like VMware, Cisco, and Nutanix, which describe the joint solutions and integrations.

4.Which three statements describe common characteristics of Cloud NGFW and VM-Series offerings? (Choose three.)

A. In Azure, both offerings can be integrated directly into Virtual WAN hubs.
B. In Azure and AWS, both offerings can be managed by Panorama.
C. In AWS, both offerings can be managed by AWS Firewall Manager.
D. In Azure, inbound destination NAT configuration also requires source NAT to maintain flow symmetry.
E. In Azure and AWS, internal (east-west) flows can be inspected without any NAT.
Answer: B, D, E
Explanation:
This question asks about common characteristics of Cloud NGFW (specifically referring to Cloud NGFW for AWS and Azure) and VM-Series firewalls.
B. In Azure and AWS, both offerings can be managed by Panorama. This is correct. Panorama is the centralized management platform for Palo Alto Networks firewalls, including both VM-Series and Cloud NGFW deployments in AWS and Azure. Panorama allows for consistent policy management, logging, and reporting across these different deployment models.
D. In Azure, inbound destination NAT configuration also requires source NAT to maintain flow symmetry. This is accurate specifically within the Azure environment. Due to how Azure networking functions, when performing destination NAT (DNAT) for inbound traffic to resources behind a firewall (whether VM-Series or Cloud NGFW), it's typically necessary to also implement source NAT (SNAT) to ensure return traffic follows the same path. This maintains flow symmetry and prevents routing issues. This is an Azure networking characteristic, not specific to the Palo Alto offerings themselves, but it applies to both in Azure.
E. In Azure and AWS, internal (east-west) flows can be inspected without any NAT. This is generally true. For traffic within the same Virtual Network (Azure) or VPC (AWS), both VM-Series and Cloud NGFW can inspect traffic without requiring NAT. This is a key advantage for microsegmentation and internal security. The firewalls can act as transparent security gateways for internal traffic.
Why other options are incorrect:
A. In Azure, both offerings can be integrated directly into Virtual WAN hubs. While VM-Series firewalls can be integrated into Azure Virtual WAN hubs as secured virtual hubs, Cloud NGFW for Azure is not directly integrated into Virtual WAN hubs in the same way. Cloud NGFW for Azure uses a different architecture, deploying as a service within a virtual network.
C. In AWS, both offerings can be managed by AWS Firewall Manager. AWS Firewall Manager is a service for managing AWS WAF, AWS Shield, and network firewalls (AWS Network Firewall). While AWS Firewall Manager can be used to manage AWS Network Firewall, it is not the management plane for Palo Alto Networks VM-Series or Cloud NGFW for AWS. These are managed by Panorama. Palo Alto Networks
Reference: To validate these points, refer to the following documentation areas on the Palo Alto Networks support site (live.paloaltonetworks.com):
Panorama Administrator's Guide: This guide details the management capabilities of Panorama, including managing VM-Series and Cloud NGFW deployments in AWS and Azure.
Cloud NGFW for AWS/Azure Documentation: This documentation outlines the architecture and deployment models of Cloud NGFW, including its management and integration with cloud platforms. VM-Series Deployment Guides for AWS/Azure: These guides describe the deployment and configuration of VM-Series firewalls in AWS and Azure, including networking considerations and integration with cloud services.

5.When registering a software NGFW to the deployment profile without internet access (i.e., offline registration), what information must be provided in the customer support portal?
A. Authcode and serial number of the VM-Series firewall
B. Hypervisor installation ID and software version
C. Number of data plane and management plane interfaces
D. CPUID and UUID of the VM-Series firewall
Answer: A
Explanation:
The question is about offline registration of a software NGFW (specifically VM-Series) when there's no internet connectivity.
A. Authcode and serial number of the VM-Series firewall: This is the correct answer. For offline registration, you need to generate an authorization code (authcode) from the Palo Alto Networks Customer Support Portal. This authcode is tied to the serial number of the VM-Series firewall. You provide both the authcode and the serial number to complete the offline registration process on the firewall itself.
Why other options are incorrect:
B. Hypervisor installation ID and software version: While the hypervisor and software version are relevant for the overall deployment, they are not the specific pieces of information required in the customer support portal for generating the authcode needed for offline registration.
C. Number of data plane and management plane interfaces: The number of interfaces is a configuration detail on the firewall itself and not information provided during the offline registration process in the support portal.
D. CPUID and UUID of the VM-Series firewall: While UUID is important for VM identification, it is not used for generating the authcode for offline registration. The CPUID is also not relevant in this context. The authcode is specifically linked to the serial number.