PassQueen
a.k.a dumpsqueen.com

Palo Alto Networks Systems Engineer Professional - Software Firewall

Palo Alto Networks PSE-SWFW-Pro-24

Version Demo

Total Demo Questions: 10

Total Premium Questions: 105

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Plan and Design	59
Topic 2, Deploy and Configure	45
Topic 3, Operate	1
Total	105

QUESTION NO: 1

Which tool can automate the deployment of VM-Series next-generation firewalls into supported public cloud service provider (CSP) environments?

A. Panorama

B. Terraform Automated Config agent

C. Public Cloud Manager (PCM) tenant

D. Docker Swarm

ANSWER: B

Explanation:

Terraform Automated Config agent is the correct choice because Terraform provides infrastructure-as-code automation for deploying the cloud resources required by VM-Series firewalls, such as virtual machines, interfaces, routing components, load balancers, public IP addresses, and cloud networking constructs. Palo Alto Networks publishes Terraform modules and examples that allow teams to define these deployments declaratively and apply them consistently across supported cloud environments. This approach makes deployments repeatable, version controlled, and suitable for CI/CD workflows, rather than requiring each firewall and its surrounding infrastructure to be provisioned manually.

In a VM-Series deployment workflow, Terraform can provision both the CSP infrastructure and the firewall instance parameters needed for bootstrap or automated initial configuration. The configuration can then be supplied through supported bootstrap mechanisms and integrated with centralized firewall policy management where required. This is particularly useful for scalable architectures, including standardized hub-and-spoke, transit, or autoscaling firewall designs, because the same code can be reused for development, testing, and production environments. Palo Alto Networks maintains reusable Terraform content for its cloud security and VM-Series deployment scenarios in its Terraform Modules GitHub repository. See also the VM-Series documentation for supported cloud deployment and automation guidance.

QUESTION NO: 2

A security team is deploying Cloud NGFW for AWS resources for several application environments. The team needs one reusable security-policy baseline that can be applied across multiple Cloud NGFW resources, while allowing environment-specific rules to remain separate.

Which Cloud NGFW for AWS object should be used for the reusable baseline policy?

A. Global Rulestack

B. Local Rulestack

C. Cloud NGFW Tenant

D. Gateway Load Balancer endpoint

ANSWER: A

Explanation:

A **Global Rulestack** is intended for reusable policy that can be associated with multiple Cloud NGFW for AWS resources. It is appropriate for common controls such as approved outbound application access, threat-prevention profiles, and organization-wide deny rules. A Local Rulestack is associated with a specific Cloud NGFW resource and is better suited to resource-specific policy requirements.

QUESTION NO: 3

A systems engineer (SE) is informed by the primary contact at a bank of an unused balance of 15,000 software NGFW flexible credits the bank does not want to lose when they expire in 1.5 years. The SE is told that the bank's new risk and

compliance officer is concerned that its operation is too permissive when allowing its servers to send traffic to SaaS vendors. Currently, its AWS and Azure VM-Series firewalls only use Advanced Threat Prevention.

What should the SE recommend to address the customer's concerns?

A. Activate Advanced WildFire within the software NGFW deployment profiles, starting with the largest vCPU models and working down to the smallest to protect their biggest workloads.

B. Subscribe to DNS Security, Advanced URL Filtering, and Advanced WildFire across all software NGFW deployment profiles until all the credits are used.

C. Verify conformance to standards and regulations, the risk of failure, and the criticality of each workload to be protected, then determine which deployment profile subscriptions address the needs.

D. Activate Advanced WildFire within the software NGFW deployment profiles, starting with the smallest vCPU models and working up to the largest to provide coverage for more VPCs and VNets with their current credit balance.

ANSWER: C

Explanation:

Verify conformance to standards and regulations, the risk of failure, and the criticality of each workload to be protected, then determine which deployment profile subscriptions address the needs. This is the appropriate recommendation because the bank has both a business constraint—using credits before expiration—and a security and governance requirement: reducing unnecessary permissiveness for server access to SaaS services. The SE should first identify the applicable regulatory obligations, the sensitivity and business impact of each protected workload, and the risk associated with its outbound traffic patterns. That assessment provides a defensible basis for selecting the subscriptions and deployment profiles that deliver the required controls rather than consuming credits without a defined security outcome.

For example, workloads that need controls over web and SaaS destinations may require URL-based policy enforcement and visibility, while DNS-related risk may call for DNS protections. Palo Alto Networks positions Advanced URL Filtering as a control for web access and URL-based threats, and DNS Security as protection against malicious and risky DNS activity. Mapping such capabilities to documented workload risk, compliance requirements, and criticality lets the bank use its flexible credits purposefully while establishing an auditable, least-privilege-oriented security posture.

QUESTION NO: 4

Which two software firewall types can protect egress traffic from workloads attached to an Azure vWAN hub? (Choose two.)

A. Cloud NGFW

B. PA-Series

C. CN-Series

D. VM-Series

ANSWER: A D

Explanation:

Cloud NGFW and **VM-Series** can protect internet-bound (egress) traffic for workloads connected through an Azure Virtual WAN hub. Cloud NGFW for Azure is a managed Palo Alto Networks firewall service designed for Azure-native deployments. Its Virtual WAN integration supports deployment in a secured vWAN hub, allowing hub-connected virtual networks to send traffic to the firewall for advanced security inspection and controlled egress. This provides centralized protection without requiring customers to operate the firewall infrastructure themselves.

VM-Series is Palo Alto Networks' virtualized next-generation firewall and can be deployed as a network virtual appliance in Azure. In a vWAN design, routing can steer traffic from connected VNets through the VM-Series firewall before it leaves the Azure environment. The firewall then applies Security policy, App-ID, threat prevention, URL filtering, and other NGFW controls to that egress flow. Both firewall types therefore provide viable architectures for centralized inspection of workload egress traffic attached to an Azure vWAN hub. Palo Alto Networks documents the Cloud NGFW vWAN integration at Cloud

NGFW for Azure in a Virtual WAN hub and VM-Series Azure deployment guidance at Set Up the VM-Series Firewall on Azure.

QUESTION NO: 5

An automation platform registers IP-to-tag mappings for short-lived cloud workloads. A Security policy rule references a Dynamic Address Group that uses those tags as membership criteria.

Which two statements describe this design? (Choose two.)

A. Dynamic tag registrations can update Dynamic Address Group membership at runtime.

B. The XML API can register IP-address-to-tag mappings.

C. Each dynamic tag registration requires a firewall commit before it is evaluated.

D. A static address object must be created for every dynamically registered workload.

E. Dynamic Address Groups can be referenced only in NAT policy rules.

ANSWER: A B

Explanation:

Dynamic tags are runtime IP-address-to-tag registrations, so a Dynamic Address Group can update its membership as registered workload IP addresses change. The XML API can register and unregister these mappings without a commit for every registration change. In contrast, the Dynamic Address Group definition and the Security policy that references it are configuration objects and must be committed when they are created or changed.

QUESTION NO: 6

Which three capabilities and characteristics are shared by the deployments of Cloud NGFW for Azure and VM-Series firewalls? (Choose three.)

A. Panorama management

B. Inter-VNet inspection through Virtual WAN hub

C. Transparent inspection of private-to-private east-west traffic that preserves client source IP address

D. Inter-VNet inspection through a transit VNet

E. Use of routing intent policies to apply security policies

ANSWER: A C D

Explanation:

Cloud NGFW for Azure and VM-Series firewalls share key deployment and traffic-inspection capabilities when used to secure Azure network environments. **Panorama management** is shared because Panorama can centrally manage policy and configuration for supported Cloud NGFW for Azure deployments as well as VM-Series firewalls, allowing security teams to apply consistent controls across their estate. Both products also support **transparent inspection of private-to-private east-west traffic that preserves client source IP address**. Preserving the original private source address is important for maintaining application visibility, logging accuracy, and policy decisions while traffic is inspected between Azure workloads. Finally, both support **inter-VNet inspection through a transit VNet**. A transit design places the firewall function on the path between connected virtual networks, enabling centralized security enforcement for traffic moving across VNet boundaries. These shared capabilities let organizations select either a managed Cloud NGFW service or a VM-Series deployment while retaining common centralized-management and east-west segmentation patterns. Palo Alto Networks documents Cloud NGFW for Azure deployment and management capabilities in its Cloud NGFW for Azure documentation and Azure deployment patterns for the virtual appliance in its VM-Series on Azure documentation.

QUESTION NO: 7

When using VM-Series firewall bootstrapping, which three methods can be used to install licensed content, including antivirus, applications, and threats? (Choose three.)

A. Panorama 10.2 or later to use the content auto push feature

B. Complete bootstrapping and either Azure Blob storage or Amazon S3 bucket

C. Content-Security-Policy update URL in the init-cfg.txt file

D. Custom-AMI or Azure VM image, with content preloaded

E. Panorama software licensing plugin

ANSWER: A B D

Explanation:

Licensed content can be made available to a bootstrapped VM-Series firewall through several supported deployment workflows. **Panorama 10.2 or later to use the content auto push feature** is correct because Panorama can centrally automate content delivery to managed firewalls, allowing required dynamic-update content to be installed without separately handling each firewall. **Complete bootstrapping and either Azure Blob storage or Amazon S3 bucket** is also correct because these cloud-storage locations can provide the bootstrap package and its content components to cloud-deployed VM-Series instances. This supports automated, repeatable deployment of the licensed antivirus, Applications and Threats, and related content packages. **Custom-AMI or Azure VM image, with content preloaded** is correct because a prepared custom image can contain the needed content before an instance is launched, which reduces post-launch update activity and helps ensure consistent content versions across a scaled deployment. These approaches are particularly useful when firewall instances must become operational quickly and with an approved baseline. Palo Alto Networks documents bootstrap package handling for VM-Series firewalls at Bootstrap the VM-Series Firewall and describes centralized content management in the Panorama centralized license management documentation.

QUESTION NO: 8

Which three statements describe the functionality of Dynamic Address Groups and tags? (Choose three.)

A. Static tags are part of the configuration on the firewall, while dynamic tags are part of the runtime configuration.

B. Dynamic Address Groups that are referenced in Security policies must be committed on the firewall.

C. To dynamically register tags, use either the XML API or the VM Monitoring agent on the firewall or on the User-ID agent.

D. IP-Tag registrations to Dynamic Address Groups must be committed on the firewall after each change.

E. Dynamic Address Groups use tags as filtering criteria to determine their members, and filters do not use logical operators.

ANSWER: A B C

Explanation:

Static tags are part of the configuration on the firewall, while dynamic tags are part of the runtime configuration. Static tags are configured locally and are associated with address objects in the candidate/running configuration. In contrast, dynamic tags are registered at runtime with IP-address-to-tag mappings. This distinction lets policy enforcement react to changing endpoint, workload, or threat-context information without requiring an administrator to edit address objects each time membership changes.

Dynamic Address Groups that are referenced in Security policies must be committed on the firewall because the Dynamic Address Group definition and its use in a Security policy are configuration elements. A commit installs those configured policy and group definitions into the running configuration so the firewall can evaluate traffic against the group.

To dynamically register tags, use either the XML API or the VM Monitoring agent on the firewall or on the User-ID agent. PAN-OS supports runtime IP-to-tag registration through the XML API, including registration via a User-ID agent, while VM

Monitoring sources can automatically identify monitored virtual-machine attributes and apply matching dynamic tags. A Dynamic Address Group evaluates its configured tag-based filter against these runtime registrations, enabling its member list to update automatically. See Use Dynamic Address Groups in Policy and Register IP Addresses and Tags Dynamically.

QUESTION NO: 9

Per reference architecture, which default PAN-OS configuration should be overridden to make VM-Series firewall deployments in the public cloud more secure?

A. Intrazone-default rule action and logging

B. Intrazone-default rule service

C. Interzone-default rule action and logging

D. Interzone-default rule service

ANSWER: A

Explanation:

Intrazone-default rule action and logging is correct. PAN-OS evaluates the intrazone-default rule when traffic does not match a more specific rule and both the source and destination are in the same security zone. Its default behavior is permissive, which is convenient for initial connectivity but is not an appropriate catch-all posture for a public-cloud deployment. A cloud zone can contain workloads with different trust levels, application roles, or network segments; therefore, same-zone classification alone should not be treated as authorization for unrestricted communication.

The VM-Series public-cloud reference architectures apply least-privilege policy design by overriding the intrazone default behavior, typically changing its action to deny and attaching logging or a Log Forwarding profile. This ensures that only explicitly defined, required east-west and north-south flows are allowed. Logging the default-policy matches also provides visibility into unexpected traffic and helps administrators identify flows that require a deliberately scoped Security policy rule. Palo Alto Networks documents the function and default handling of Security policy rules in its Security Policy documentation and recommends a deny-by-default, explicitly permitted policy posture in its Internet Gateway Best Practices.

QUESTION NO: 10

A Cloud NGFW for AWS deployment is being inserted into workload traffic by using AWS Gateway Load Balancer. The cloud network team must update VPC route tables so that protected traffic is transparently forwarded to the managed firewall service.

Which AWS component is used as the route-table target for this traffic insertion?

A. Gateway Load Balancer endpoint

B. Internet gateway

C. Amazon S3 gateway endpoint

D. Network ACL

ANSWER: A

Explanation:

A **Gateway Load Balancer endpoint** is the VPC route-table target used to steer traffic to a Gateway Load Balancer service. Cloud NGFW for AWS uses Gateway Load Balancer endpoints for transparent traffic insertion. The endpoint is deployed in a subnet and provides the attachment point through which traffic is forwarded for inspection.