PassQueen
a.k.a dumpsqueen.com

Palo Alto Networks System EngineerPrisma CloudProfessional

Palo Alto Networks PSE-Prisma-Pro-24

Version Demo

Total Demo Questions: 10

Total Premium Questions: 105

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

In which two ways can Prisma Cloud Compute (PCC) edition be installed? (Choose two.)

A. self-managed in a customer's own container platform

B. self-contained hardware appliance

C. as a stand-alone Windows application

D. Cloud-hosted as part of a Prisma Cloud Enterprise tenant from Palo Alto Networks

ANSWER: A D

Explanation:

Prisma Cloud Compute supports both self-hosted and SaaS deployment models. In a self-managed deployment, the organization deploys and operates the Prisma Cloud Compute Console in its own environment, typically on its container platform. This model gives the customer operational control over the Console environment while allowing Defenders to protect supported hosts, containers, Kubernetes environments, serverless workloads, and cloud resources.

Prisma Cloud Compute capabilities can also be consumed through a cloud-hosted Prisma Cloud Enterprise tenant operated by Palo Alto Networks. In this SaaS model, Palo Alto Networks hosts the Prisma Cloud Console service, while the customer configures protection and deploys the required Defenders into the environments being secured. These deployment choices let organizations select an operating model that aligns with their infrastructure, administrative requirements, and responsibility boundaries. Palo Alto Networks documents the Compute architecture and its Console/Defender components at Prisma Cloud Compute architecture. The available Prisma Cloud editions and SaaS service model are described at Prisma Cloud.

QUESTION NO: 2

Amazon Web Services WAF can be enabled on which two resources?(Choose two.)

A. AWS CDN

B. AWS NAT Gateway

C. AWS ALB

D. AWS NLB

ANSWER: A C

Explanation:

AWS CDN, referring to an Amazon CloudFront distribution, and **AWS ALB**, referring to an Application Load Balancer, are supported AWS WAF protected resources. AWS WAF is associated with a web ACL, which supplies rules that inspect and control incoming HTTP(S) web requests. A web ACL can be associated with a CloudFront distribution to filter requests at AWS edge locations before they reach the origin. This is a common way to apply centralized protections, such as managed rule groups, IP-based restrictions, and rate-based rules, to content delivered through a CDN. AWS WAF can also be associated with an Application Load Balancer. In this deployment, the web ACL evaluates requests sent to applications behind the load balancer and can allow, block, count, or apply CAPTCHA/challenge actions according to the configured rules. CloudFront web ACLs use the CloudFront scope, whereas an Application Load Balancer uses a Regional web ACL in the same AWS Region as the load balancer. These associations make both services suitable enforcement points for Layer 7 web-application protection. See the AWS WAF documentation on associating a web ACL with AWS resources and the AWS WAF Developer Guide.

QUESTION NO: 3

An administrator has deployed an AWS transit gateway and used multiple VPC spokes to segregate a multi-tier application. The administrator also created a security VPC with multiple VM-Series NGFWs in an active/active deployment model via ECMP using Amazon Web Services VPN-based attachments.

What must be configured on the firewall to avoid asymmetric routing?

A. source address translation

B. destination address translation

C. port address translation

D. source and destination address translation

ANSWER: A

Explanation:

source address translation must be configured on the VM-Series firewalls. With an AWS Transit Gateway using ECMP over VPN attachments, traffic from a spoke VPC can be distributed across multiple equal-cost VPN tunnels and firewalls. The firewall that establishes a session must also receive the return traffic for that session, because the VM-Series is stateful and keeps the session state locally rather than sharing it across independent active/active instances.

Source NAT translates the original spoke workload address to an address associated with the firewall handling the flow. Return traffic is then addressed back to that translated source, allowing AWS routing and the VPN attachment design to deliver the response through the same firewall that created the session. This preserves bidirectional session symmetry while retaining ECMP scale for separate flows. Palo Alto Networks specifically documents source NAT as the requirement for avoiding asymmetric routing when deploying VM-Series firewalls with Transit Gateway ECMP and VPN attachments.

See the Palo Alto Networks Transit Gateway with VPN Attachments deployment guide and the NAT administration documentation.

QUESTION NO: 4 - (SIMULATION)

A customer has deployed a VM-Series NGFW on Amazon Web Services using a PAYG license. What is the sequence required by the customer to switch to a BYOL license?

ANSWER: Check the explanation for the answer

Explanation:

Required sequence:

1. **Back up** the configuration from the PAYG VM-Series firewall.
2. **Register** the BYOL authorization code/licenses to the customer's Palo Alto Networks Support Portal account.
3. **Deploy** a new VM-Series firewall using the AWS BYOL AMI (the PAYG instance is not converted in place).
4. **Activate** the BYOL licenses on the newly deployed firewall.
5. **Load** (restore/import) the saved configuration onto the BYOL firewall.

In short: `Backup → Register → Deploy → Activate → Load`.

QUESTION NO: 5

What are two benefits of Cloud Security Posture Management (CSPM) over other solutions? (Choose two.)

A. guaranteed proof of concept (POC) extensions beyond 30 days

B. native integration of network, endpoint, and cloud data to stop attacks

C. elimination of blind spots

D. proactive addressing of risks

ANSWER: C D

Explanation:

elimination of blind spots is a core CSPM benefit because CSPM continuously discovers and assesses cloud assets, configurations, identities, and services across cloud environments. This centralized, ongoing visibility helps security teams identify unmanaged resources, configuration drift, and exposures that might otherwise remain outside normal security monitoring. Prisma Cloud CSPM provides asset inventory, configuration assessment, and policy-based visibility to establish a more complete view of cloud risk.

proactive addressing of risks is also correct because CSPM evaluates cloud configurations against security best practices, compliance frameworks, and organizational policies before a misconfiguration can contribute to an incident. It prioritizes findings and supports remediation workflows so teams can correct excessive permissions, publicly exposed resources, missing encryption, and other risky conditions early in the development or operational lifecycle. This shifts cloud security from a reactive investigation model to continuous prevention and posture improvement. Palo Alto Networks describes CSPM as providing continuous visibility and compliance monitoring for cloud environments, while Prisma Cloud documentation details its policy-driven configuration and posture-management capabilities. See Palo Alto Networks Cloud Security Posture Management and Prisma Cloud CSPM documentation.

QUESTION NO: 6

Which statement explains the correlation between the block and alert thresholds in a vulnerability management policy?

A. The thresholds can be set to informational, low, medium, high, and critical.

B. The alert threshold always has precedence over, and can be greater than, the block threshold.

C. The block threshold must always be equal to or greater than the alert threshold.

D. The block threshold always has precedence over, and can be less than, the alert threshold.

ANSWER: C

Explanation:

The block threshold must always be equal to or greater than the alert threshold. In a Prisma Cloud vulnerability management policy, the alert threshold determines the vulnerability severity at which Prisma Cloud generates an alert, while the block threshold determines the severity at which the configured enforcement action prevents the workload or image from proceeding. Blocking is the stronger enforcement outcome, so its configured threshold cannot be lower than the alerting threshold in the policy's severity ordering. This relationship supports a consistent escalation path: vulnerabilities first meet the policy's notification criteria and, at the same or a more severe level, meet its prevention criteria. For example, a policy can alert and block at the same severity, or alert on a broader range of findings while reserving blocking for findings of greater severity. This configuration model lets teams gain visibility into risk before applying the most disruptive enforcement action, while still ensuring that vulnerabilities meeting the organization's blocking standard are handled automatically. Palo Alto Networks documents vulnerability policy configuration and enforcement behavior in its Vulnerability Management Policies documentation and the Prisma Cloud Compute Vulnerability Management documentation.

QUESTION NO: 7

A team clones a default Prisma Cloud policy because it needs to change the policy logic for an internal control. The original default policy is mapped to a compliance standard. After the clone is enabled, what must the team do if the custom policy results are to contribute to that compliance standard?

A. Associate the cloned policy with the applicable compliance-standard requirement.

B. Disable the original policy and enable the cloned policy.

C. Edit the original default policy to use the custom RQL logic.

D. Create a notification template for the cloned policy.

ANSWER: A

Explanation:

The team must **associate the cloned custom policy with the applicable requirement in the compliance standard**. A cloned policy is a separate custom policy with its own logic and lifecycle. Its findings do not automatically replace the findings of the original policy in an existing compliance-standard mapping.

Enabling the cloned policy makes it available for evaluation but does not change compliance mappings. Editing the original default policy is not the appropriate customization workflow, and creating a new notification template affects alert delivery rather than compliance scoring.

QUESTION NO: 8

An administrator uses Prisma Cloud account groups to separate production cloud accounts from development accounts. Which two outcomes can account groups support? (Choose two.)

A. Scope alert rules to a defined set of cloud accounts.

B. Control user access to a defined set of cloud accounts.

C. Create network segmentation between cloud accounts.

D. Modify cloud-provider IAM permissions for grouped accounts.

E. Replace policies with account-specific configuration checks.

ANSWER: A B

Explanation:

Account groups can be used to **scope alert rules** so that selected policies evaluate only the intended cloud accounts. They can also be used to **control user access to cloud accounts**, allowing administrators to delegate visibility and management responsibilities by account grouping.

An account group does not create cloud-provider network segmentation or change IAM permissions in AWS, Azure, or Google Cloud. It also does not replace a Prisma Cloud policy; policies still define the security condition being evaluated.

QUESTION NO: 9

A Kubernetes platform team deploys Prisma Cloud Compute Container Defenders by using a DaemonSet. The deployment is rejected by the cluster security controls because the Defender requires access to host-level runtime information. What is the most appropriate remediation?

A. Allow the Defender DaemonSet to use the required privileged access and host mounts.

B. Deploy the Defender as an unprivileged application Deployment.

C. Replace the Defender DaemonSet with a Kubernetes Ingress resource.

D. Update the Console credentials used by the Defender.

ANSWER: A

Explanation:

The team must allow the Container Defender deployment to use the **required privileged access and host mounts**. Container Defender requires host-level visibility to protect containers running on a Kubernetes node, and the DaemonSet deployment therefore uses permissions and mounts that restrictive pod-security controls can deny.

Deploying the Defender as a normal application workload does not provide node-level protection. Replacing the DaemonSet with an Ingress resource does not deploy runtime protection, and changing only the Console credentials does not address the Kubernetes admission failure.

QUESTION NO: 10

Which pillar of the Prisma Cloud platform can secure outbound traffic, stop lateral attack movement, and block inbound threats?

A. Cloud Workload Protection (CWP)

B. Cloud Code Security

C. Cloud Network Security

D. Cloud Identity Security

ANSWER: C

Explanation:

Cloud Network Security is the Prisma Cloud platform pillar designed to protect cloud network traffic across its full path: inbound traffic entering cloud environments, east-west traffic moving between workloads, and outbound traffic leaving workloads or cloud networks. It applies next-generation firewall capabilities and cloud-native network controls to inspect traffic, enforce policy, and prevent threats. This enables organizations to block malicious inbound connections, restrict unauthorized lateral movement that attackers may use to reach additional resources, and control egress traffic to reduce data-exfiltration and command-and-control risk. Prisma Cloud Network Security brings these protections together for public-cloud environments, including virtualized and containerized workloads, while providing centralized visibility and policy enforcement. Palo Alto Networks describes its cloud network security capabilities as protecting applications and workloads from network-based threats through segmentation, threat prevention, and secure connectivity. These functions directly align with securing outbound traffic, stopping lateral movement, and blocking inbound threats. See Palo Alto Networks' Prisma Cloud Network Security overview and the Prisma Cloud Network Security documentation.