PassQueen
a.k.a dumpsqueen.com

Palo Alto Networks System Engineer Professional - SASE Exam

Palo Alto Networks PSE-SASE

Version Demo

Total Demo Questions: 8

Total Premium Questions: 88

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, SASE	34
Topic 2, Prisma Access	29
Topic 3, Prisma SD-WAN	13
Topic 4, Autonomous Digital Experience Management (ADEM)	10
Topic 5, CloudBlades	2
Total	88

QUESTION NO: 1

Which two statements describe Security Profile Groups? (Choose two.)

A. They combine multiple Security Profiles into one reusable object.

B. They can be attached to a Security policy rule.

C. They replace the need for Security policy rules.

D. They provide IP address-to-user mapping.

ANSWER: A B

Explanation:

A Security Profile Group can **combine multiple Security Profiles into one reusable object** and can **be attached to a Security policy rule**. This simplifies policy administration because an administrator can assign a consistent set of inspection controls, such as Antivirus, Anti-Spyware, Vulnerability Protection, and URL Filtering, through a single profile-group reference.

Using profile groups helps ensure that similar allow rules receive the same security posture and reduces the effort required to update a common set of profiles across multiple policy rules. Palo Alto Networks documents profile groups and their use with Security policy rules in the Security Profile Groups documentation.

QUESTION NO: 2

Which two security controls can be applied to allowed internet-bound traffic by attaching Security Profiles to a Security policy rule? (Choose two.)

A. Antivirus

B. Vulnerability Protection

C. Zone Protection

D. Interface Management Profile

ANSWER: A B

Explanation:

Antivirus and **Vulnerability Protection** profiles can be attached to an allow rule to inspect permitted traffic for malware and exploit attempts. Antivirus profiles detect and block supported malware patterns in network traffic, while Vulnerability Protection profiles detect exploits targeting known vulnerabilities. Applying these profiles to allow rules is a core best practice because permitted sessions require inspection before they reach users or applications.

Zone Protection is applied to a zone rather than attached as a Security Profile to an individual Security policy rule. Palo Alto Networks documents Security Profiles and their use with Security policy in the Security Profiles documentation.

QUESTION NO: 3

Which type of access allows unmanaged endpoints to access secured on-premises applications?

A. manual external gateway

B. secure web gateway (SWG)

C. GlobalProtect VPN for remote access

D. Prisma Access Clientless VPN

ANSWER: D

Explanation:

Prisma Access Clientless VPN is designed to provide browser-based, agentless access to authorized private applications for users on unmanaged or third-party endpoints. Instead of requiring the GlobalProtect app or a full network-layer VPN tunnel on the device, the user authenticates through a web browser and accesses published internal web applications through Prisma Access. This model is particularly appropriate when an organization cannot install or manage endpoint software, such as on contractor-owned, kiosk, partner, or personally owned devices.

Clientless VPN supports secure access controls by integrating authentication and authorization with the organization's identity and security policies. Administrators explicitly define the applications and resources made available, helping provide least-privilege access rather than broad network connectivity. For access to secured on-premises applications, Prisma Access connects the service to private resources through the organization's service connections, while the clientless portal acts as the controlled access point for the unmanaged endpoint. Palo Alto Networks describes Clientless VPN as enabling secure remote access to internal web applications without requiring endpoint software. See the Prisma Access Clientless VPN documentation and the Palo Alto Networks secure access overview.

QUESTION NO: 4

Which three decryption methods are available in a security processing node (SPN)? (Choose three.)

A. SSL Outbound Proxy

B. SSHv2 Proxy

C. SSL Forward Proxy

D. SSL Inbound Inspection

E. SSH Inbound Inspection

ANSWER: B C D

Explanation:

The available SPN decryption methods are **SSHv2 Proxy**, **SSL Forward Proxy**, and **SSL Inbound Inspection**. SSL Forward Proxy decrypts outbound TLS traffic initiated by internal users, allowing the security processing node to inspect the application content and apply Security policy enforcement before re-encrypting traffic for its destination. SSL Inbound Inspection decrypts inbound TLS sessions for services hosted behind the protected environment; it uses the protected server's certificate and private key to inspect encrypted traffic directed to that server. SSHv2 Proxy enables inspection and control of Secure Shell version 2 connections, including SSH tunneling activity, so that security policy can be applied to traffic carried through the SSH session. These methods reflect the PAN-OS decryption capabilities used by Prisma Access security processing nodes to provide visibility into encrypted traffic while enforcing threat prevention and access-control policy. Palo Alto Networks documents SSL Forward Proxy and SSL Inbound Inspection as the principal TLS decryption deployment types and describes SSH Proxy as the supported method for decrypting SSHv2 sessions. See the Palo Alto Networks Decryption Overview and Configure SSH Proxy.

QUESTION NO: 5

Which product allows advanced Layer 7 inspection, access control, threat detection and prevention?

A. Infrastructure as a Service (IaaS)

B. remote browser isolation

C. network sandbox

D. Firewall as a Service (FWaaS)

ANSWER: D

Explanation:

Firewall as a Service (FWaaS) is correct because it delivers cloud-based, next-generation firewall security controls for users and traffic regardless of where they connect. In Palo Alto Networks Prisma SASE, FWaaS applies advanced Layer 7 inspection through App-ID, which identifies and controls applications based on their actual behavior rather than relying only on ports and protocols. It also provides access control through granular security policies, allowing organizations to define which applications, users, destinations, and content are permitted. Threat detection and prevention are provided through integrated security capabilities such as Threat Prevention, URL Filtering, WildFire analysis, DNS Security, and Advanced Threat Prevention. This combination lets security teams consistently inspect traffic, enforce policy, and stop malicious activity for branches, remote users, and cloud-delivered connectivity without depending on a traditional on-premises firewall deployment. Palo Alto Networks describes Prisma Access FWaaS as a cloud-delivered security service that includes next-generation firewall capabilities and centrally managed security policy enforcement. This makes Firewall as a Service (FWaaS) the product that directly fulfills all the functions named in the question: Layer 7 visibility and control, access control, and threat prevention. See the Prisma Access documentation and Palo Alto Networks' FWaaS overview.

QUESTION NO: 6

Which action protects against port scans from the internet?

A. Apply App-ID Security policy rules to block traffic sourcing from the untrust zone.

B. Assign Security profiles to Security policy rules for traffic sourcing from the untrust zone.

C. Apply a Zone Protection profile on the zone of the ingress interface.

D. Assign an Interface Management profile to the zone of the ingress surface.

ANSWER: C

Explanation:

Apply a Zone Protection profile on the zone of the ingress interface. A Zone Protection profile is designed to defend the firewall at the network-zone level from reconnaissance and flood-style attacks that can occur before traffic is evaluated by ordinary Security policy rules. In its Reconnaissance Protection settings, Palo Alto Networks provides scan protection controls, including port scan detection, which identify hosts that probe multiple ports in a configured interval and can block the offending source for a specified duration. For scans arriving from the public internet, the profile must be applied to the external/untrust security zone associated with the interface receiving that inbound traffic. This placement is important because Zone Protection is evaluated for traffic entering the protected zone, allowing the firewall to detect and mitigate the scanning behavior at the perimeter. Administrators can tune the alert, activate, and maximum thresholds to match normal traffic patterns and reduce false positives while retaining effective protection against hostile reconnaissance. Palo Alto Networks documents Zone Protection as the mechanism for protecting against reconnaissance attacks such as port scans and host sweeps. See Zone Protection and Configure Zone Protection.

QUESTION NO: 7

An organization uses multiple cloud-managed security services and requires a centralized method to synchronize directory information and map users to groups for policy enforcement.

Which service should be configured?

A. Cloud Identity Engine

B. Cortex Data Lake

C. CloudBlades

D. Advanced WildFire

ANSWER: A

Explanation:

Cloud Identity Engine is the correct service because it provides a cloud-based identity infrastructure for integrating identity providers and directories with Palo Alto Networks cloud-managed services. It can synchronize user and group information so that administrators can use group-based policy consistently across supported services, including Prisma Access. This reduces the need to configure and maintain separate directory integrations for each enforcement point.

Cloud Identity Engine supports identity-aware security policy by making directory and group information available to the cloud-delivered management environment. See the Cloud Identity Engine documentation for configuration and integration details.

QUESTION NO: 8

Which two point products are consolidated into the Prisma secure access service edge (SASE) platform? (Choose two.)

A. Autonomous Digital Experience Management (ADEM)

B. firewall as a service (FWaaS)

C. Threat Intelligence Platform (TIP)

D. security information and event management (SIEM)

ANSWER: A B

Explanation:

Autonomous Digital Experience Management (ADEM) and firewall as a service (FWaaS) are integrated capabilities within the Prisma SASE platform. ADEM provides end-to-end visibility into a user's digital experience by continuously measuring application, network, and device performance. This enables operations teams to identify whether poor experience originates in the endpoint, local network, internet path, SaaS application, or the security service, and to remediate issues more quickly. Palo Alto Networks delivers these experience insights as part of the Prisma SASE operational model rather than requiring a separate monitoring workflow.

Firewall as a service (FWaaS) is delivered through Prisma Access and supplies cloud-delivered, next-generation firewall enforcement for users, branches, and applications. It applies consistent security controls such as threat prevention, URL filtering, malware protection, and policy enforcement regardless of user location. Consolidating FWaaS with ADEM in Prisma SASE lets organizations combine secure connectivity, cloud-delivered inspection, and experience monitoring under a unified SASE architecture and management approach. Palo Alto Networks describes Prisma SASE as converging networking and security services while including ADEM capabilities for monitoring and improving digital experience. See the Prisma SASE overview and the ADEM product overview.