DUMPSARENA

Palo Alto Networks Systems Engineer (PSE) - Strata Associate

Palo Alto Networks PSE-Strata-Associate

Version Demo

Total Demo Questions: 5

Total Premium Questions: 57

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

What is a technical benefit of User-ID in relation to policy control?

A. It matches traffic against policy to check whether it is allowed on the network.

B. It allows all users to designate view-only access to itinerant personnel.

C. It improves safe enablement of applications traversing the network.

D. It encrypts all private keys and passwords in the configuration.

ANSWER: C

Explanation:

It improves safe enablement of applications traversing the network. User-ID maps network activity to known users and groups rather than relying only on IP addresses, which can be dynamic, shared, or otherwise insufficient to identify who initiated a connection. This identity context can be used directly in Security policy rules alongside application, service, source and destination zones, addresses, and other match criteria. As a result, administrators can permit a specific business application for only the users or directory groups with a legitimate need, while applying appropriate security controls to that access. This supports least-privilege policy design and gives security teams clearer visibility into which users are using applications on the network. Palo Alto Networks describes User-ID as a feature that enables policy enforcement and visibility based on user and group identity, including integration with directory services. Combining user identity with App-ID therefore allows applications to be enabled in a controlled, identity-aware manner rather than broadly for every device on a subnet. See the Palo Alto Networks User-ID documentation and the Palo Alto Networks App-ID overview.

QUESTION NO: 2

The ability of a Next-Generation Firewall (NGFW) to logically group physical and virtual interfaces and then control traffic based on that grouping is known as what?

A. LLDP profiles

B. security zones

C. DHCP groups

D. security profile groups

ANSWER: B

Explanation:

Security zones are the logical groupings used by Palo Alto Networks NGFWs to organize one or more physical, virtual, aggregate, or subinterfaces according to their trust level, network role, or traffic-handling requirements. An interface is assigned to a zone, and Security policy rules then identify the source zone and destination zone for traffic. This zone-based model lets an administrator apply consistent access-control decisions to traffic regardless of the specific interface on which the traffic enters or exits the firewall. For example, multiple interfaces serving internal networks can be placed in an internal zone, while an internet-facing interface can be assigned to an untrust zone. Rules can then permit, inspect, or deny traffic between those logical groups. Zone membership is therefore a core part of defining policy scope and segmentation on the firewall. Palo Alto Networks documentation describes security zones as logical groupings of interfaces and explains that policy rules use source and destination zones to control traffic. See Security Zones and Configure Layer 3 Interfaces.

QUESTION NO: 3

Which of the following is an appropriate first step for a customer interested in moving to Zero Trust?

A. Ask administrators to switch on the Zero Trust options and features of their current products.

B. Secure the funding required to incorporate the new architecture into their existing networks.

C. Set priorities by identifying the most valuable and critical assets and data on their networks.

D. Request a statement of compliance from their IT vendors against the Zero Trust standard.

ANSWER: C

Explanation:

Set priorities by identifying the most valuable and critical assets and data on their networks. This is an appropriate first step because Zero Trust is a strategic security approach that is implemented incrementally around what the organization must protect most. Before selecting controls or changing architecture, the customer needs to understand its high-value data, business-critical applications, sensitive systems, users, and workflows. This inventory establishes the protection priorities and provides the context needed to define policies that continuously verify access based on identity, device posture, application, data sensitivity, and risk.

Palo Alto Networks describes Zero Trust as an approach built on explicit verification, least-privileged access, and assuming breach. Applying these principles effectively requires knowing which resources have the greatest business value and which access paths reach them. Focusing first on critical assets also helps the customer create a practical roadmap, start with manageable use cases, and measure risk reduction as protections are expanded. This aligns with the protect-surface-oriented method used in Zero Trust planning rather than treating Zero Trust as a single feature to enable. See Palo Alto Networks: What Is Zero Trust Architecture? and NIST SP 800-207: Zero Trust Architecture.

QUESTION NO: 4

In which two of the following scenarios is personal data excluded from protection under the General Data Protection Regulation (GDPR)?

Select 2 Correct Responses

A. The data was automated as part of an information filing system.

B. The data was generated in the course of a purely personal or household activity.

C. The data will be used for the prevention of criminal offenses.

D. The data is related to a person ' s economic or cultural identity.

ANSWER: B C

Explanation:

The data was generated in the course of a purely personal or household activity is excluded because the GDPR does not apply to processing performed by a natural person in the course of activities that are genuinely personal or household in nature. This exemption covers activity with no connection to a professional or commercial activity, such as maintaining a private address book or personal social interactions. The scope is set out in Article 2(2)(c) of the GDPR.

The data will be used for the prevention of criminal offenses is excluded from the GDPR where the processing is carried out by competent authorities for the prevention, investigation, detection, or prosecution of criminal offences, including safeguarding against and preventing threats to public security. Article 2(2)(d) directs such law-enforcement processing outside the GDPR's scope; it is instead addressed at EU level by the Law Enforcement Directive. The exclusion depends on the legally defined law-enforcement purpose and competent-authority context, not merely a general statement that data may be useful in relation to crime.

These exclusions are expressly defined in the GDPR's material scope provisions. See GDPR, Article 2 and Directive (EU) 2016/680.

QUESTION NO: 5

An administrator wants to deploy a pair of firewalls in an active/active high availability (HA) architecture.

Which two deployment types are supported in this circumstance? (Choose two.) Select 2 Correct Responses

A. Layer 3

B. TAP mode

C. Virtual Wire

D. Layer 2

ANSWER: A C

Explanation:

Active/active HA is supported for **Layer 3** and **Virtual Wire** deployments. In an active/active design, both peers can process traffic, and the firewalls use HA session synchronization plus forwarding mechanisms to maintain consistent traffic handling across the pair. Layer 3 deployments support this model because the firewalls can route traffic while coordinating ownership and session state. Virtual Wire deployments also support active/active HA, allowing the pair to operate transparently inline while sharing session information and using the active/active forwarding design.

When designing either supported deployment, interfaces, zones, routing or virtual-wire configuration, HA links, and session synchronization must be planned consistently on both peers. Palo Alto Networks also recommends carefully considering asymmetric traffic and selecting the appropriate active/active forwarding method so packets belonging to the same session are handled correctly. The platform documentation identifies Layer 3 and Virtual Wire as the deployment modes available for active/active HA. See the Palo Alto Networks HA modes documentation and the Palo Alto Networks knowledge base article.