Vendor: Palo Alto Networks

Exam Code: NetSec-Architect

Exam Name: Palo Alto Network Security Architect

Version: DEMO

QUESTION 1
A retail organization wants to sanction the use of a particular third-party SaaS-based AI application for inventory management. This application will need network layer data access to the organization's internal supply chain database with confidential information highly secured in its own DMZ. The implementation is delayed because the CISO is concerned that the sanctioned third-party AI application could get compromised and then used to exfiltrate customer PH from the internal database. Which solution will address the CISO's concern?

A. Prisma AIRS with the AI agent deployed on the database server to monitor for unauthorized access attempts
B. Prisma AIRS with AI Security content updates to inspect the model's behavior and block anomalous database queries
C. AI Access Security with an App-ID Cloud Engine subscription to precisely identify and then block the inventory management application entirely
D. AI Access Security with an Enterprise DLP subscription to identify and block the PII within the traffic to and from the SaaS application

Answer: D
Explanation:
Enterprise DLP integrated with AI Access Security inspects traffic to and from the SaaS application and can detect sensitive data such as customer PII. It enforces policies to prevent exfiltration even if the application is compromised, allowing the organization to safely sanction the AI application while protecting confidential data.

QUESTION 2
Which factor must be taken into consideration when determining whether an NGFW edge architecture or a SASE architecture is appropriate to recommend to a customer planning to implement a Zero Trust Network Access (ZTNA) solution?

A. ZTNA requires User-ID and Group-ID information that is not available in Prisma SD-WAN
B. ZTNA can be implemented regardless of the whether an NGFW or SASE solution is selected
C. ZTNA revolves around an agent on the endpoint and does not influence the overall NGFW or SASE architecture
D. ZTNA is a component of SASE and can only be implemented with Prisma Access

Answer: B
Explanation:
Zero Trust Network Access is a security approach that can be implemented using either traditional NGFW-based architectures or SASE solutions. The key consideration is how identity, policy enforcement, and segmentation are applied, not the deployment model itself, since both architectures are capable of supporting ZTNA principles.

QUESTION 3
An organization has selected Prisma SD-WAN ION devices for use at branch offices and is working to build a low-level design for its sites. A typical branch site has a 10 Mbps MPLS with fiber LC-SR, and an RJ-45 Ethernet 50 Mbps DIA internet circuit.

There are 75 workstations and a stacked core switch that supports LACP, M-LAG, BGP, and OSPF will be used. The core switch is the default gateway for all local VLANs. The final design will determine the selection of the appropriate model and accessories for the site.

Which statement applies to the Prisma SD-WAN architecture in this use case?

A. MPLS underlay paths cannot be used as an active path alongside internet overlay path
B. Connectivity over the MPLS will be lost when the device that terminates it loses power
C. High availability (HA) for the LAN side connectivity can at most support two interfaces using LAG / LACP
D. Only a default route can be advertised on a LAN-side BGP peering from the ION

Answer: B
Explanation:
In this design, the MPLS circuit is being terminated by the ION. If that device loses power, the MPLS path also goes down because the branch loses the device that is physically terminating and forwarding that private WAN connection. Prisma SD-WAN does support using private WAN and internet paths actively, so the issue is not coexistence of MPLS and DIA. It also supports LAN-side BGP beyond just advertising a default route, and LAG/LACP can bundle multiple LAN interfaces rather than being limited to only two.

QUESTION 4
An architect is designing a security solution for a large AWS environment with numerous application virtual private clouds (VPCs). These applications have diverse and sometimes conflicting inbound security requirements, making a single, unified ruleset challenging to create and maintain. The solution must secure inbound traffic for different application groups while also centrally securing all outbound and east-west traffic via an AWS Transit Gateway. Which design model recommendation will simplify rule complexity for inbound traffic while meeting all security requirements?

A. Transit Gateway model focused on establishing connectivity by creating a full mesh of direct peering connections between all application VPCs
B. Combined model using dedicated inbound NGFWs for logical application groups and a central NGFW for east-west and outbound traffic
C. Isolated model deploying a separate non-connected security VPC for each application VPC
D. Centralized model to consolidating all security functions by directing all inbound, outbound, and east-west traffic through a single, shared security VPC

Answer: B
Explanation:
A combined model is designed for environments where inbound requirements differ across application groups. It uses dedicated inbound firewalls for those logical application groups, which keeps inbound policy sets simpler and easier to manage, while a central NGFW tied to the Transit Gateway secures outbound and east-west traffic centrally. Palo Alto Networks documents this combined deployment pattern specifically as using inbound security at the application VPC side and the transit gateway as the hub for east-west and outbound security.

QUESTION 5
A security architect needs to design a log collection architecture for a large organization with hundreds of firewalls distributed across multiple geographic regions. The primary requirement is to ensure that if a single Log Collector in any region fails, logs from the firewalls in that region will automatically be sent to another available Log Collector without manual intervention. What is the recommended Panorama feature to achieve this level of log collection resilience?

A. Log Collector Group for each geographic region
B. Storage capacity increase on each individual Log Collector
C. Load balancer to distribute logs across all Log Collectors
D. Log Collectors deployed in a high availability (HA) pair

Answer: A
Explanation:
A Log Collector Group allows multiple collectors to operate together so firewalls can automatically forward logs to any available collector in the group. If one collector fails, logging seamlessly continues to other members without manual reconfiguration, providing the required resilience across regions.

QUESTION 6
A technology company is deploying its own AI applications on a Google Kubernetes Engine (GKE) cluster. The development team is concerned about protecting the complex, microservices-based AI stack from both internal and external threats: such as data poisoning and lateral movement between containerized components. Which solution should be proposed to address these concerns?

A. AI Access Security with Advanced URL Filtering
B. AI Access Security with App-ID Cloud Engine
C. Prisma AIRS Network Intercept
D. Prisma AIRS API Intercept

Answer: C
Explanation:
Network Intercept provides visibility and enforcement on east-west and north-south traffic within Kubernetes environments, allowing inspection of communications between microservices. This enables detection and prevention of threats such as lateral movement and data poisoning by analyzing runtime network behavior inside the AI application stack.

QUESTION 7
An architect is reviewing a use case with the following requirements:

```
- Visibility on the health of an end user's path for the five most
critical applications
- Metrics on the impact of endpoint health for application
- Centralized call quality analytics from Zoom video conferencing
solution
- Insights into the supporting protocols, such as DNS
- Support 600 users on Windows desktops in a single sales office
```

Which solution should be recommended to meet these requirements?

A. Remote networks with ADEM enabled and an ION device
B. GlobalProtect with a Prisma Access portal configured and ADEM enabled
C. Prisma SD-WAN using the native application dashboard and link quality monitoring
D. Prisma Browser or the Prisma Browser extension with RUM metrics

Answer: A
Explanation:
ADEM with a remote network and an ION device is the best fit for a single office deployment because it provides end-to-end visibility for branch users and applications, including path monitoring for critical apps and insight into supporting services such as DNS. Palo Alto Networks also states that ADEM for remote sites is supported on Prisma SD-WAN remote sites with ION platforms, and ADEM's Zoom integration delivers centralized meeting quality analytics correlated with network and endpoint factors. This aligns with the requirement to monitor user experience for

a 600-user Windows-based sales office from a centralized view.

QUESTION 8
A large organization uses Palo Alto Networks VM-Series firewalls deployed across multiple availability zones in Microsoft Azure. These are managed by an Azure Virtual Machine Scale Set (VMSS) and integrated with an Azure Load Balancer for high availability (HA) traffic inspection within a Transit VNet.

The security team needs to perform a critical PAN-OS software upgrade across the entire fleet of firewalls with the requirement of minimal application downtime.

Following Palo Alto Networks best practices for highly available cloud deployments, what is the recommended approach for safely performing this software upgrade with the least downtime?

A. Update the image in an Azure VMSS and then initiate an upgrade of the instances
B. Configure Azure Load Balancer probes to handle the health check failover during upgrades
C. Provision a new, parallel VMSS with the new PAN-OS version, validate it, and redirect traffic from the old VMSS to the new one
D. Use Azure Update Manager to push the PAN-OS upgrade package directly to all firewall instances simultaneously during a scheduled maintenance window

Answer: C
Explanation:
The safest approach with the least downtime is a blue/green-style replacement: build a new parallel VMSS running the target PAN-OS version, validate it fully, and then redirect traffic from the old scale set to the new one. Palo Alto Networks documents creating custom Azure VM-Series images for the exact PAN-OS version you want to deploy, which supports standing up a separate validated fleet rather than in-place upgrading the active inspection path. Azure health probes help determine instance health during updates, but they do not remove the risk of service disruption from upgrading the live fleet in place.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**