



TRUSTED, ACCURATE AND RELIABLE!

The most comprehensive IT certification
preparation materials in the industry!

All rights reserved. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. Unauthorized copying, reselling, or distribution of this document is strictly prohibited and may result in legal action.

<https://www.virtulearner.com>
support@virtulearner.com

Palo Alto Networks

PSE-Strata-Pro-24

Palo Alto Networks Systems

Engineer Professional -

Hardware Firewall

QUESTION: 1

A company plans to deploy identity for improved visibility and identity-based controls for least privilege access to applications and data

A. The company does not have an on-premises Active Directory (AD) deployment, and devices are connected and managed by using a combination of Entra ID and Jamf.

Which two supported sources for identity are appropriate for this environment? (Choose two.)

B. Captive portal

C. User-ID agents configured for WMI client probing

D. GlobalProtect with an internal gateway deployment

E. Cloud Identity Engine synchronized with Entra ID

Answer(s): C, D

Explanation:

In this scenario, the company does not use on-premises Active Directory and manages devices with Entra ID and Jamf, which implies a cloud-native and modern management setup. Below is the evaluation of each option:

Option A: Captive portal

Captive portal is typically used in environments where identity mapping is needed for unmanaged devices or guest users. It provides a mechanism for users to authenticate themselves through a web interface.

However, in this case, the company is managing devices using Entra ID and Jamf, which means identity information can already be centralized through other means. Captive portal is not an ideal solution here.

This option is not appropriate.

Option B: User-ID agents configured for WMI client probing

WMI (Windows Management Instrumentation) client probing is a mechanism used to map IP addresses to usernames in a Windows environment. This approach is specific to on-premises Active Directory deployments and requires direct communication with Windows endpoints.

Since the company does not have an on-premises AD and is using Entra ID and Jamf, this method is not applicable.

This option is not appropriate.

Option C: GlobalProtect with an internal gateway deployment

GlobalProtect is Palo Alto Networks' VPN solution, which allows for secure remote access. It also supports identity-based mapping when deployed with internal gateways.

In this case, GlobalProtect with an internal gateway can serve as a mechanism to provide user and device visibility based on the managed devices connecting through the gateway.

This option is appropriate.

Option D: Cloud Identity Engine synchronized with Entra ID

The Cloud Identity Engine provides a cloud-based approach to synchronize identity information from identity providers like Entra ID (formerly Azure AD).

In a cloud-native environment with Entra ID and Jamf, the Cloud Identity Engine is a natural fit as it integrates seamlessly to provide identity visibility for applications and data.

This option is appropriate.

Reference:

Palo Alto Networks documentation on Cloud Identity Engine

GlobalProtect configuration and use cases in Palo Alto Knowledge Base

QUESTION: 2

A systems engineer (SE) is working with a customer that is fully cloud-deployed for all applications. The customer is interested in Palo Alto Networks NGFWs but describes the following challenges:

"Our apps are in AWS and Azure, with whom we have contracts and minimum-revenue guarantees. We would use the built-in firewall on the cloud service providers (CSPs), but the need for centralized policy management to reduce human error is more important."

Which recommendations should the SE make?

- A. Cloud NGFWs at both CSPs; provide the customer a license for a Panorama virtual appliance from their CSP's marketplace of choice to centrally manage the systems.
- B. Cloud NGFWs in AWS and VM-Series firewall in Azure; the customer selects a PAYG licensing Panorama deployment in their CSP of choice.
- C. VM-Series firewalls in both CSPs; manually built Panorama in the CSP of choice on a host of either type: Palo Alto Networks provides a license.
- D. VM-Series firewall and CN-Series firewall in both CSPs; provide the customer a private-offer Panorama virtual appliance from their CSP's marketplace of choice to centrally manage the systems.

Answer(s): A

Explanation:

The customer is seeking centralized policy management to reduce human error while maintaining compliance with their contractual obligations to AWS and Azure. Here's the evaluation of each option:

Option A: Cloud NGFWs at both CSPs; provide the customer a license for a Panorama virtual appliance from their CSP's marketplace of choice to centrally manage the systems