Palo Alto Networks

PSE-STRATA-PRO-24 Exam

Palo Alto Networks Systems Engineer Professional - Hardware Firewall

Questions & Answers
Demo

Version: 4.0

Question: 1

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

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.)

A. Captive portal

B. User-ID agents configured for WMI client probing

C. GlobalProtect with an internal gateway deployment

D. Cloud Identity Engine synchronized with Entra ID

Answer: 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: 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

Cloud NGFW is a fully managed Next-Generation Firewall service by Palo Alto Networks, offered in AWS and Azure marketplaces. It integrates natively with the CSP infrastructure, making it a good fit for customers with existing CSP agreements.

Panorama, Palo Alto Networks' centralized management solution, can be deployed as a virtual appliance in the CSP marketplace of choice, enabling centralized policy management across all

NGFWs.

This option addresses the customer's need for centralized management while leveraging their existing contracts with AWS and Azure.

This option is appropriate.

Option B: Cloud NGFWs in AWS and VM-Series firewall in Azure; the customer selects a PAYG licensing Panorama deployment in their CSP of choice

This option suggests using Cloud NGFW in AWS but VM-Series firewalls in Azure. While VM-Series is a flexible virtual firewall solution, it may not align with the customer's stated preference for CSP-managed services like Cloud NGFW.

This option introduces a mix of solutions that could complicate centralized management and reduce operational efficiency.

This option is less appropriate.

Option 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

VM-Series firewalls are well-suited for cloud deployments but require more manual configuration compared to Cloud NGFW.

Building a Panorama instance manually on a host increases operational overhead and does not leverage the customer's existing CSP marketplaces.

This option is less aligned with the customer's needs.

Option 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

This option introduces both VM-Series and CN-Series firewalls in both CSPs. While CN-Series firewalls are designed for Kubernetes environments, they may not be relevant if the customer does not specifically require container-level security.

Adding CN-Series firewalls may introduce unnecessary complexity and costs.

This option is not appropriate.

Reference:

Palo Alto Networks documentation on Cloud NGFW

Panorama overview in Palo Alto Knowledge Base

VM-Series firewalls deployment guide in CSPs: Palo Alto Documentation

Question: 3

A customer claims that Advanced WildFire miscategorized a file as malicious and wants proof, because another vendor has said that the file is benign.

How could the systems engineer assure the customer that Advanced WildFire was accurate?

A. Review the threat logs for information to provide to the customer.

B. Use the WildFire Analysis Report in the log to show the customer the malicious actions the file took when it was detonated.

C. Open a TAG ticket for the customer and allow support engineers to determine the appropriate action.

D. Do nothing because the customer will realize Advanced WildFire is right.

Answer: B

Explanation:

Advanced WildFire is Palo Alto Networks' cloud-based malware analysis and prevention solution. It determines whether files are malicious by executing them in a sandbox environment and observing their behavior. To address the customer's concern about the file categorization, the systems engineer must provide evidence of the file's behavior. Here’s the analysis of each option:

Option A: Review the threat logs for information to provide to the customer

Threat logs can provide a summary of events and verdicts for malicious files, but they do not include the detailed behavior analysis needed to convince the customer.

While reviewing the logs is helpful as a preliminary step, it does not provide the level of proof the customer needs.

This option is not sufficient on its own.

Option B: Use the WildFire Analysis Report in the log to show the customer the malicious actions the file took when it was detonated

WildFire generates an analysis report that includes details about the file's behavior during detonation in the sandbox, such as network activity, file modifications, process executions, and any indicators of compromise (IoCs).

This report provides concrete evidence to demonstrate why the file was flagged as malicious. It is the most accurate way to assure the customer that WildFire's decision was based on observed malicious actions.

This is the best option.

Option C: Open a TAG ticket for the customer and allow support engineers to determine the appropriate action

While opening a support ticket is a valid action for further analysis or appeal, it is not a direct way to assure the customer of the current WildFire verdict.

This option does not directly address the customer’s request for immediate proof.

This option is not ideal.

Option D: Do nothing because the customer will realize Advanced WildFire is right

This approach is dismissive of the customer's concerns and does not provide any evidence to support WildFire's decision.

This option is inappropriate.

Reference:

Palo Alto Networks documentation on WildFire

WildFire Analysis Reports

Question: 4

Which three known variables can assist with sizing an NGFW appliance? (Choose three.)

A. Connections per second

B. Max sessions

C. Packet replication

D. App-ID firewall throughput

E. Telemetry enabled

Answer: A, B, D

Explanation:

When sizing a Palo Alto Networks NGFW appliance, it's crucial to consider variables that affect its performance and capacity. These include the network's traffic characteristics, application requirements, and expected workloads. Below is the analysis of each option:

Option A: Connections per second

Connections per second (CPS) is a critical metric for determining how many new sessions the firewall can handle per second. High CPS requirements are common in environments with high traffic turnover, such as web servers or applications with frequent session terminations and creations.

This is an important sizing variable.

Option B: Max sessions

Max sessions represent the total number of concurrent sessions the firewall can support. For environments with a large number of users or devices, this metric is critical to prevent session exhaustion.

This is an important sizing variable.

Option C: Packet replication

Packet replication is used in certain configurations, such as TAP mode or port mirroring for traffic inspection. While it impacts performance, it is not a primary variable for firewall sizing as it is a specific use case.

This is not a key variable for sizing.

Option D: App-ID firewall throughput

App-ID throughput measures the firewall's ability to inspect traffic and apply policies based on application signatures. It directly impacts the performance of traffic inspection under real-world conditions.

This is an important sizing variable.

Option E: Telemetry enabled

While telemetry provides data for monitoring and analysis, enabling it does not significantly impact the sizing of the firewall. It is not a core variable for determining firewall performance or capacity.

This is not a key variable for sizing.

Reference:

Palo Alto Networks documentation on Firewall Sizing Guidelines

Knowledge Base article on Performance and Capacity Sizing

Question: 5

Which statement applies to the default configuration of a Palo Alto Networks NGFW?

A. Security profiles are applied to all policies by default, eliminating implicit trust of any data traversing the firewall.

B. The default policy action for intrazone traffic is deny, eliminating implicit trust within a security zone.

C. The default policy action allows all traffic unless explicitly denied.

D. The default policy action for interzone traffic is deny, eliminating implicit trust between security zones.

Answer: D

Explanation:

The default configuration of a Palo Alto Networks NGFW includes a set of default security rules that determine how traffic is handled when no explicit rules are defined. Here's the explanation for each option:

Option A: Security profiles are applied to all policies by default, eliminating implicit trust of any data

traversing the firewall

Security profiles (such as Antivirus, Anti-Spyware, and URL Filtering) are not applied to any policies by default. Administrators must explicitly apply them to security rules.

This statement is incorrect.

Option B: The default policy action for intrazone traffic is deny, eliminating implicit trust within a security zone

By default, traffic within the same zone (intrazone traffic) is allowed. For example, traffic between devices in the "trust" zone is permitted unless explicitly denied by an administrator.

This statement is incorrect.

Option C: The default policy action allows all traffic unless explicitly denied

Palo Alto Networks firewalls do not have an "allow all" default rule. Instead, they include a default "deny all" rule for interzone traffic and an implicit "allow" rule for intrazone traffic.

This statement is incorrect.

Option D: The default policy action for interzone traffic is deny, eliminating implicit trust between security zones

By default, traffic between different zones (interzone traffic) is denied. This aligns with the principle of zero trust, ensuring that no traffic is implicitly allowed between zones. Administrators must define explicit rules to allow interzone traffic.

This statement is correct.

Reference:

Palo Alto Networks documentation on Security Policy Defaults

Knowledge Base article on Default Security Rules