DUMPSARENA

Palo Alto Networks Systems Engineer ProfessionalHardware Firewall

Palo Alto Networks PSE-Strata-Pro-24

Version Demo

Total Demo Questions: 8

Total Premium Questions: 83

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

A customer has acquired 10 new branch offices, each with fewer than 50 users and no existing firewall. The systems engineer wants to recommend a PA-Series NGFW with Advanced Threat Prevention at each branch location. Which NGFW series is the most cost-efficient at securing internet traffic?

A. PA-200

B. PA-400

C. PA-500

D. PA-600

ANSWER: B

Explanation:

PA-400 is the appropriate choice because the PA-400 Series is built to deliver next-generation firewall protection for distributed enterprise branches and small offices while maintaining an economical hardware footprint. For branch locations with fewer than 50 users, this series provides sufficient performance to inspect internet-bound traffic with Palo Alto Networks security subscriptions, including Advanced Threat Prevention, without sizing the deployment for the substantially greater capacity generally required at larger sites.

The PA-400 platform runs PAN-OS and supports the same policy-based security architecture and cloud-delivered security services used across the PA-Series portfolio. This allows each newly acquired branch to receive consistent application-aware controls, threat prevention inspection, and centralized operational management while keeping both appliance and deployment costs appropriate for a small branch environment. Selecting a common PA-400 platform for all 10 sites also supports a repeatable branch design and consistent policy enforcement. Palo Alto Networks describes the series as an ML-powered next-generation firewall family for branch offices and distributed enterprise deployments; its official product information is available at PA-400 Series NGFW. Platform specifications and supported capabilities can also be reviewed in the PA-400 Hardware Reference.

QUESTION NO: 2

According to a customer's CIO, who is upgrading PAN-OS versions, "Finding issues and then engaging with your support people requires expertise that our operations team can better utilize elsewhere on more valuable tasks for the business." The upgrade project was initiated in a rush because the company did not have the appropriate tools to indicate that their current NGFWs werereaching capacity.

Which two actions by the Palo Alto Networks team offer a long-term solution for the customer? (Choose two.)

A. Recommend that the operations team use the free machine learning-powered AIOps for NGFW tool.

B. Suggest the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls.

C. Inform the CIO that the new enhanced security features they will gain from the PAN-OS upgrades will fix any future problems with upgrading and capacity.

D. Propose AIOps Premium within Strata Cloud Manager (SCM) to address the company's issues from within the existing technology.

ANSWER: B D

Explanation:

Suggesting the inclusion of training into the proposal so that the operations team is informed and confident in working on their firewalls provides a durable people-and-process solution. Training helps administrators develop the practical PAN-OS knowledge needed to plan maintenance, validate software compatibility, interpret health information, perform upgrades safely, and efficiently engage Support when an escalation is actually needed. This directly reduces the operational burden identified by the CIO and enables the team to devote more time to business priorities.

Proposing AIOps Premium within Strata Cloud Manager (SCM) addresses the technology and visibility gap that led to the rushed project. AIOps capabilities use firewall telemetry and analytics to surface operational risks, health issues, and capacity-related trends proactively. Centralized visibility and guided insights allow the organization to identify conditions that may affect firewall performance or scale before they become urgent, while also improving readiness for ongoing PAN-OS lifecycle management. Used alongside administrator training, this creates a sustainable operating model: personnel can understand and act on prioritized insights, while the platform provides proactive monitoring across the firewall environment. Palo Alto Networks describes AIOps for NGFW as delivering proactive operational insights and recommendations, and its education services support role-based firewall administration skills. See AIOps for NGFW and Palo Alto Networks Education Services.

QUESTION NO: 3

Which two compliance frameworks are included with the Premium version of Strata Cloud Manager (SCM)? (Choose two)

A. Payment Card Industry (PCI)

B. National Institute of Standards and Technology (NIST)

C. Center for Internet Security (CIS)

D. Health Insurance Portability and Accountability Act (HIPAA)

ANSWER: A B

Explanation:

Payment Card Industry (PCI) and National Institute of Standards and Technology (NIST) are included compliance frameworks in Strata Cloud Manager Premium. The Premium license provides compliance-posture capabilities that assess managed firewall configurations against predefined compliance requirements and present the findings in compliance views and reports. This gives security teams a structured way to identify configuration gaps, prioritize remediation, and provide evidence for internal governance or external audit processes.

PCI support is especially relevant to organizations that store, process, or transmit payment-card data, because it helps map firewall-policy and security-control posture to payment-card security expectations. NIST support similarly provides a recognized control-oriented framework for assessing and improving an organization's cybersecurity posture. In SCM, these frameworks complement the platform's centralized management and operational insights by turning configuration and policy data into actionable compliance findings. Palo Alto Networks documents the Premium licensing features and the compliance-related capabilities available through Strata Cloud Manager in its product documentation and licensing information: Strata Cloud Manager Documentation and Strata Cloud Manager Licensing.

QUESTION NO: 4

A company has multiple business units, each of which manages its own user directories and identity providers (IdPs) with different domain names. The company's network security team wants to deploy a shared GlobalProtect remote access service for all business units to authenticate users to each business unit ' s IdP.

Which configuration will enable the network security team to authenticate GlobalProtect users to multiple SAML IdPs?

A. GlobalProtect with multiple authentication profiles for each SAML IdP

B. Multiple Authentication Mode Cloud Identity Engine authentication profile for use on the GlobalProtect portals and gateways

C. Authentication sequence that has multiple authentication profiles using different authentication methods

D. Multiple Cloud Identity Engine tenants for each business unit

ANSWER: B

Explanation:

Multiple authentication mode Cloud Identity Engine authentication profile for use on the GlobalProtect portals and gateways is the appropriate configuration for a shared GlobalProtect deployment serving users from separate business units and SAML identity providers. Cloud Identity Engine provides a centralized identity integration layer, and its Multiple Authentication Mode capability allows a single authentication profile to present and process multiple configured authentication methods or identity-provider choices. The same profile can then be referenced by the GlobalProtect portal and gateway, allowing users to authenticate through the IdP associated with their business unit rather than requiring separate GlobalProtect services for every domain.

This design is particularly useful when the organization has decentralized identity administration but needs a common remote-access infrastructure. Each business unit can retain its own directory and SAML IdP configuration while the network security team centrally operates the portal and gateway configuration. The user's selected or applicable authentication method directs the sign-in flow to the relevant IdP, and GlobalProtect receives the resulting authenticated identity for policy enforcement and access control. Palo Alto Networks documents Cloud Identity Engine authentication profiles and their use for firewall and GlobalProtect authentication in the Configure an Authentication Profile guide. See also the GlobalProtect documentation for portal and gateway authentication configuration.

QUESTION NO: 5

A customer has created user- and group-based Security policy rules for access to sensitive internal applications. Traffic logs for several internal clients show only source IP addresses, and the expected user-based rules are not matching.

Which action should the systems engineer take first?

A. Verify that User-ID has a valid user-to-IP address mapping for each affected client.

B. Verify that the Security policy rule uses an application-default service.

C. Verify that the Log Forwarding profile includes Traffic logs.

D. Verify that a custom URL category contains the internal application address.

ANSWER: A

Explanation:

The engineer should first verify that the firewall has valid User-ID user-to-IP address mappings for the affected client IP addresses. User-based Security policy depends on the firewall associating a username with the source IP address of the session. If that mapping is absent, expired, or incorrect, the firewall cannot match the traffic against a rule that specifies a user or group.

Group mapping is also needed to resolve group membership, but it does not by itself establish the user-to-IP mapping required for traffic identification. App-ID identifies the application, and Log Forwarding profiles export logs; neither resolves a missing username in traffic logs.

QUESTION NO: 6

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

GlobalProtect with an internal gateway deployment is appropriate because GlobalProtect can authenticate users as they connect through an internal gateway and provide the firewall with user-to-IP address mappings. Those mappings allow Security policy rules and logging to use user and group identity, rather than relying only on IP addresses. This provides identity visibility for managed endpoints on the internal network without requiring an on-premises AD deployment for the mapping method itself. Palo Alto Networks documents GlobalProtect as a supported User-ID mapping source: User-ID Mapping.

Cloud Identity Engine synchronized with Entra ID is also appropriate because Cloud Identity Engine integrates with cloud identity providers, including Microsoft Entra ID, to retrieve and synchronize users and groups for identity-based policy. This directly fits an organization whose identity is cloud-native and whose endpoint management includes Entra ID and Jamf. The synchronized directory information enables the firewall and associated Palo Alto Networks services to resolve users and groups for least-privilege access controls, while avoiding a dependency on a locally deployed AD domain. Palo Alto Networks describes the Entra ID directory synchronization workflow in its Cloud Identity Engine documentation.

QUESTION NO: 7

A customer has a Vulnerability Protection profile attached to its internet-facing Security policy rule. Threat logs show repeated critical exploit attempts matching the profile, but the sessions are allowed and the server continues to receive the traffic.

Which configuration change should the systems engineer recommend?

A. Configure the matching Vulnerability Protection signature action to block or reset the session.

B. Configure the Log Forwarding profile to forward Threat logs to the SIEM.

C. Configure a WildFire Analysis profile to block the exploit attempt.

D. Configure DNS sinkholing in an Anti-Spyware profile.

ANSWER: A

Explanation:

The engineer should configure the applicable Vulnerability Protection signature action to block or reset the matching sessions and commit the updated profile. Security profiles can generate alerts without preventing traffic when their configured action is alert. The presence of Threat logs confirms that the firewall is detecting the exploit attempts, but the configured signature action determines whether the firewall permits, blocks, or resets the session.

Changing the Log Forwarding profile affects external log delivery, not inline prevention. A WildFire Analysis profile is used for file submission, and an Anti-Spyware profile addresses spyware and command-and-control detections rather than the observed vulnerability signature action.

QUESTION NO: 8

Which two statements correctly describe best practices for sizing a firewall deployment with decryption enabled? (Choose two.)

A. SSL decryption traffic amounts vary from network to network.

B. Large average transaction sizes consume more processing power to decrypt.

C. Perfect Forward Secrecy (PFS) ephemeral key exchange algorithms such as Diffie-Hellman Ephemeral (DHE) and Elliptic-Curve Diffie-Hellman Exchange (ECDHE) consume more processing resources than Rivest-Shamir-Adleman (RSA) algorithms.

D. Rivest-Shamir-Adleman (RSA) certificate authentication method (not the RSA key exchange algorithm) consumes more resources than Elliptic Curve Digital Signature Algorithm (ECDSA), but ECDSA is more secure.

ANSWER: A C

Explanation:

“SSL decryption traffic amounts vary from network to network.” is correct because decryption sizing must be based on the organization’s actual traffic profile, not simply on total interface bandwidth. The proportion of traffic using TLS, the number of concurrent sessions and new connections, application mix, cipher suites, and the percentage of traffic excluded from decryption all affect the load placed on the firewall. Palo Alto Networks recommends using observed traffic characteristics and appropriate decryption performance values when selecting a platform.

“Perfect Forward Secrecy (PFS) ephemeral key exchange algorithms such as Diffie-Hellman Ephemeral (DHE) and Elliptic-Curve Diffie-Hellman Exchange (ECDHE) consume more processing resources than Rivest-Shamir-Adleman (RSA) algorithms.” is also correct. Forward-proxy decryption requires the firewall to participate in TLS session establishment as well as inspect the resulting plaintext traffic. Ephemeral key exchanges used for PFS add cryptographic processing during connection setup, so a deployment with substantial use of DHE or ECDHE can require more capacity than one using RSA key exchange. This makes the negotiated TLS characteristics, along with real-world encrypted-traffic volume, essential inputs to a defensible sizing exercise. See Palo Alto Networks’ SSL Forward Proxy Decryption documentation and Decryption Best Practices.