DUMPSARENA

Palo Alto Networks Network Security Analyst

Palo Alto Networks NetSec-Analyst

Version Demo

Total Demo Questions: 9

Total Premium Questions: 94

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Platform and Architecture	1
Topic 2, Core Concepts	13
Topic 3, Configuration	55
Topic 4, Operations and Maintenance	25
Total	94

QUESTION NO: 1

A user receives a browser certificate error when accessing a website. The Decryption profile is configured to block sessions when the destination server certificate is expired. Which two log types should the analyst review first to confirm the certificate-validation failure and the associated session disposition? (Choose two.)

A. Decryption Log

B. Traffic Log

C. System Log

D. Configuration Log

E. Data Filtering Log

ANSWER: A B

Explanation:

The Decryption log records SSL/TLS decryption processing and certificate-validation errors, including failures caused by an expired server certificate. The Traffic log provides the related session details, such as the matched Security policy rule, application, action, source, destination, and session end reason. Together, these logs establish both the decryption failure and the firewall handling of the session.

QUESTION NO: 2

What are two valid pattern types in a Data Filtering profile? (Choose two.)

A. Custom Dictionary

B. Proximity Pattern

C. File Properties

D. Regular Expression

ANSWER: C D

Explanation:

File Properties and **Regular Expression** are valid pattern types for custom data patterns used by a PAN-OS Data Filtering profile. A Regular Expression pattern lets an administrator define text that conforms to a specified format, such as an internal identifier, project number, or other organization-specific sensitive-data value. The firewall evaluates supported file content against that expression, enabling detection of information that is not covered by built-in predefined patterns.

File Properties identifies content using document metadata rather than a text value in the body of the file. This can include properties associated with supported documents, allowing policy to recognize files based on attributes such as title, author, subject, or other metadata. These pattern types can be selected when defining a custom data pattern and then referenced in a Data Filtering profile rule, where administrators can apply alert and block thresholds according to the organization's data-protection requirements.

Palo Alto Networks documents custom data patterns as using either regular expressions or file properties, and Data Filtering profiles use those patterns to inspect and control sensitive-data transfers. See the PAN-OS Data Filtering documentation and the Data Patterns documentation.

QUESTION NO: 3

An organization uses several different web-conferencing tools (Zoom, Microsoft Teams, WebEx). The analyst wants to create a single security rule to allow all these tools without listing each App-ID individually. What should the analyst create?

A. Application Filter

B. Application Group

C. Service Group

D. Custom App-ID

ANSWER: A

Explanation:

Application Filter is correct because it dynamically matches App-IDs that share selected attributes, allowing the analyst to reference the filter once in a Security policy rule rather than manually enumerating every application. For web-conferencing and collaboration products, the analyst can build a filter using the relevant App-ID classification attributes, such as the collaboration category or applicable subcategory, and PAN-OS evaluates the applications that meet those criteria. This approach provides a scalable policy construct for an environment using multiple conferencing tools: when Palo Alto Networks adds a newly identified App-ID to the selected classification in a content update, it can automatically match the existing filter without requiring an edit to the Security rule itself. The filter can also be narrowed with additional criteria, including risk, technology, characteristics, or administrator-defined tags, so the allowed scope remains aligned with the organization's policy. Palo Alto Networks describes application filters as dynamic groupings based on application properties, whereas application groups are explicitly assembled lists of named applications. See the PAN-OS documentation on Application Filters and Application Groups.

QUESTION NO: 4

Beyond being a SaaS-based delivery platform, what is an advantage of Strata Cloud Manager (SCM) over Panorama? (Choose one answer)

A. Live, inline best practice checks

B. Real-time alerting

C. Customizable dashboards

D. NGFW and Prisma Access management

ANSWER: A

Explanation:

Live, inline best practice checks is the advantage because Strata Cloud Manager embeds security-posture guidance directly into the policy-creation and configuration workflow. Rather than treating best-practice validation as a separate assessment activity, SCM can identify configuration risks as an administrator creates or changes policy. This gives the administrator immediate, actionable feedback before deployment, helping ensure that policy design follows Palo Alto Networks guidance and that important controls are consistently applied.

This capability supports a more proactive operating model. Security teams can find and remediate issues such as unsafe policy constructs, missing recommended security controls, or configuration choices that weaken their intended Zero Trust posture while they are still working on the change. Inline guidance therefore reduces the likelihood that inconsistent or risky configurations will reach managed firewalls and makes it easier to maintain standards across a distributed environment. Palo Alto Networks describes Strata Cloud Manager as a unified cloud-delivered management experience that uses AI-driven capabilities to simplify operations and improve security outcomes. Its best-practice-oriented guidance is a meaningful workflow enhancement because it brings validation closer to the point at which policy decisions are made. See the Strata Cloud Manager product overview and the Strata Cloud Manager documentation.

QUESTION NO: 5

What is the function of a " Service " object in a Palo Alto Networks firewall configuration?

A. To define the Layer 7 App-ID signatures.

B. To define the Layer 4 protocol (TCP/UDP) and port numbers.

C. To specify the URL categories to be blocked.

D. To set the QoS priority for specific traffic.

ANSWER: B

Explanation:

To define the Layer 4 protocol (TCP/UDP) and port numbers is correct. A Service object identifies the transport protocol and destination port or port range that a security policy can use to match traffic. When creating a service, the administrator selects either TCP or UDP and configures the applicable destination port settings; source ports can also be configured when needed. This provides a reusable, consistently defined Layer 4 match criterion rather than requiring an administrator to enter port values separately in every policy.

Service objects are especially useful for applications or services that must be permitted on explicitly defined ports, including internally hosted applications using nonstandard ports. They can be referenced directly in Security policy rules or collected in Service Groups, which lets administrators apply a common set of services across policies and update membership centrally. In Security policy configuration, the service setting also supports predefined choices such as *application-default*, which restricts allowed applications to their standard ports, while custom Service objects provide the precise TCP or UDP port definitions needed for exceptions. Palo Alto Networks documents Service objects as port-based definitions and distinguishes them from application identification, URL filtering, and QoS configuration. See the Palo Alto Networks Service Objects documentation and the Security Policy rule matching documentation.

QUESTION NO: 6

Before enabling SSL Forward Proxy Decryption for employee web traffic, which two actions are required to prevent browsers from reporting that the firewall-generated certificates are untrusted? (Choose two.)

A. Configure a certificate on the firewall for Forward Trust use.

B. Deploy the issuing CA certificate to endpoint trusted certificate stores.

C. Import the private key for every external web server into the firewall.

D. Configure SSL Inbound Inspection for all internet destinations.

E. Create a Destination NAT rule for outbound HTTPS traffic.

ANSWER: A B

Explanation:

SSL Forward Proxy requires the firewall to present a substitute certificate to the client. The firewall must have a certificate configured for Forward Trust use, and endpoints must trust the certificate authority that issued that certificate. Deploying the issuing CA certificate to managed endpoint trust stores allows browsers to validate certificates generated by the firewall. The private key of every external web server is neither available nor required for Forward Proxy Decryption.

QUESTION NO: 7

Several Security policy rules reference the same Security Profile Group. An analyst updates the Antivirus profile that is a member of that group and commits the change. What is the expected result?

A. All rules that reference the Security Profile Group use the updated Antivirus profile after the commit.

B. Each Security policy rule must be edited to select the updated Antivirus profile.

C. Only new Security policy rules can use the updated Antivirus profile.

D. The change takes effect only after the next antivirus content update.

ANSWER: A

Explanation:

All Security policy rules that reference the Security Profile Group use the updated Antivirus profile after the configuration is committed. A Security Profile Group provides reusable, centralized association of multiple Security profiles to policy rules, so administrators do not need to edit every rule individually when a member profile changes.

The policy rules do not need to be recreated or individually reassigned. The change does not affect rules that use a different profile group or have individually assigned profiles. A content update is separate from a configuration commit and is not sufficient to apply an administrator's profile-setting change.

QUESTION NO: 8

Which object type allows an analyst to group multiple IP addresses based on their geographical location (country) to simplify "Geo-blocking" policies?

A. Static Address Object

B. FQDN Address Object

C. Regions

D. Dynamic Address Group (DAG)

ANSWER: C

Explanation:

Regions is the correct object type because a Palo Alto Networks firewall can use its IP-address geolocation database to associate public IP addresses with countries and other geographic areas. A region object lets an analyst select one or more countries and then use that object directly in the source or destination address field of a Security policy. The firewall evaluates the IP address against its maintained geolocation mappings, so the policy can consistently apply a geographic access-control requirement without an administrator having to build and maintain individual address entries for all IP networks assigned to each country.

This is particularly useful for geo-blocking, where an organization may want to deny inbound traffic from countries in which it has no users, customers, partners, or business operations. It also makes rules more readable and easier to update: the policy expresses the intended geographic scope, while content updates help keep the underlying IP-to-location information current. Region objects can contain multiple countries, enabling a single reusable object to represent an approved or restricted geographic set across multiple policies. Palo Alto Networks documents geographic region objects and their use in policy configuration in its PAN-OS administrator documentation: Enable Policy to Use IP Address Geolocation and Addresses.

QUESTION NO: 9

A user reports that an upload to an approved web application was stopped. The Security policy rule permits the application and includes a Data Filtering profile. Which two log types should the analyst review to confirm the sensitive-data match and the session-level policy disposition? (Choose two.)

A. Threat Log

B. System Log

C. Data Filtering Log

D. Decryption Log

E. Traffic Log

ANSWER: C E

Explanation:

The **Data Filtering log** records events generated when configured data patterns are detected and includes information about the matching pattern and enforcement action. The **Traffic log** provides the session-level context, including the matched Security policy rule, application, source and destination information, and session disposition.

Threat logs are used for security-profile detections such as vulnerability, spyware, antivirus, and file-related threat events. Decryption logs are useful when investigating TLS decryption processing, but they do not identify a Data Filtering pattern match. System logs record firewall operational and configuration events rather than the affected user session.