PRACTICE TEST SOFTWARE

Palo Alto Networks

NetSec-Analyst Exam

Palo Alto Networks Network Security Analyst

DEMO Version

Full Version Features:

• 90 Days Free Updates

• 30 Days Money Back Guarantee

• Instant Download Once Purchased

• 24 Hours Live Chat Support

Full version is available at link below with affordable price.

https://www.practicetestsoftware.com/palo-alto-networks/netsec-analyst

Question 1. (Single Select)

Which action ensures that a Panorama push will not fail due to pending local firewall changes?

A: Commit configurations locally on the device and then repeat the same configuration from Panorama.
B: Disable "Merge with Device Candidate Config."
C: Enable "Force Template Values."
D: Enable both options "Include Device and Network Templates" and "Include Firewall Clusters."

Correct Answer: B

Explanation:
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
In a Palo Alto Networks environment managed by Panorama, synchronization between the management server and the managed firewalls is critical. When an administrator performs a "Push to Devices," Panorama attempts to merge the template and device group configurations with the candidate configuration currently residing on the local firewall's control plane.
If there are pending local changes—meaning an administrator has made manual changes directly on the firewall GUI or CLI that have not yet been committed—the Panorama push will often fail. This safeguard exists because Panorama, by default, attempts to merge its push with the existing candidate configuration on the device to prevent accidental overwrites or configuration conflicts. To bypass this specific failure point, the analyst must disable "Merge with Device Candidate Config" in the Panorama Push window. When this option is unchecked, Panorama ignores the local candidate configuration and pushes only the Panorama-defined settings.
It is a core objective for a Network Security Analyst to maintain Panorama as the "Source of Truth" for the security posture. While Option C (Force Template Values) ensures that Panorama's template settings override local settings during the push, it does not specifically address the block caused by a "dirty" candidate configuration session on the managed device. Therefore, disabling the merge functionality ensures the push process can complete without being blocked by uncommitted local administrative sessions, maintaining operational continuity across the network fabric.

Question 2. (Multi Select)

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

Correct Answer: C, D

Explanation:

Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:

In the Palo Alto Networks ecosystem, specifically when utilizing Strata Cloud Manager (SCM) and Enterprise Data Loss Prevention (DLP), Data Filtering profiles are used to identify and protect sensitive information. When an analyst creates a custom data pattern to be used within these profiles, the system allows for two primary methods of identification: Regular Expressions (Regex) and File Properties.

Regular Expressions (D) allow the analyst to define a specific string or numerical pattern, such as a custom employee ID format or a proprietary project code. This is the most flexible and common way to catch sensitive text data within a file or data stream.

File Properties (C) allow the analyst to create patterns based on the metadata or attributes of a file rather than its contents. This includes identifying files based on the "Author," "Title," "Company," or even custom tags embedded in document properties (e.g., Microsoft Word or PDF metadata). By combining these two pattern types, a Network Security Analyst can create a highly granular detection engine. For instance, a policy could block any file where the "Company" property is set to a competitor or any file containing text that matches a specific Regex-defined sensitive data format.

While "Predefined" patterns (like Credit Card numbers) are also a core component, they are not listed as an option here. "Proximity Patterns" are a feature used to reduce false positives by ensuring two patterns appear near each other, but the fundamental "pattern types" for custom definitions are Regex and File Properties.

Question 3. (Single Select)

A security analyst is using the Strata Cloud Manager (SCM) Policy Optimizer to create specific and focused rules. The analyst accepts the new rules from Policy Optimizer and updates the rule base, but the traffic does not hit these new rules.

Which action needs to be taken to resolve this issue?

A: Execute a push configuration

B: Remove the original Security policy rule

C: Enable the newly created Security policy rules

D: Perform a commit

Correct Answer: D

Explanation:

Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:

In the Palo Alto Networks management workflow—whether using a local firewall, Panorama, or Strata Cloud Manager (SCM)—there is a fundamental distinction between the Candidate Configuration and the Running Configuration. When an analyst uses the Policy Optimizer to identify applications and "clones" or creates new App-ID based rules, these changes are initially written only to the Candidate Config.

The reason the traffic does not hit the new rules immediately is that the firewall's data plane is still operating based on the last successful Running Configuration. In the context of SCM or Panorama, even after "accepting" the rules in the interface, the changes remain in a staged state. To move these changes from the management plane to the active inspection engine, the analyst must Perform a commit.

A commit validates the configuration syntax and compiles the new policy into the hardware's lookup tables. Without a commit, the new rules effectively do not exist in the eyes of the traffic processing engine. While "Execute a push configuration" (Option A) is a valid step in a Panorama-to-Firewall workflow, the term Commit is the universal required action to activate local candidate changes. Furthermore, even if the rules are created, the firewall evaluates rules from top to bottom; however, the most common reason for new rules appearing "invisible" to traffic immediately after creation in the GUI is the lack of a finalized commit.

Question 4. (Single Select)

Which log type should be checked first using Log Viewer when a user reports being unable to access a specific website?

A: Firewall/URL

B: Firewall/Traffic

C: Firewall/Threat

D: Firewall/DNS Security

Correct Answer: B

Explanation:

Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:

When troubleshooting connectivity issues, such as a user being unable to access a website, the Traffic Log is the primary starting point for any Palo Alto Networks Network Security Analyst. The Traffic Log provides the most fundamental view of the communication attempt, showing whether a session was even initiated and how the firewall handled it.

By searching the Traffic Log (using filters for the source IP of the user or the destination URL/IP), an analyst can immediately see the Action taken by the firewall—whether it was allow, deny, or drop. Crucially, it reveals the Rule Name that the traffic hit. If the action is deny, the analyst knows the issue is likely a missing or misconfigured Security policy. If the action is allow but the user still can't connect, the analyst looks at the Type column (e.g., end vs. deny) and the Session End Reason. For example, an end reason of policy-deny confirms a policy block, while tcp-rst-from-server might indicate a problem with the web server itself rather than the firewall.

While URL Logs or Threat Logs (Options A and C) provide more specific detail if a Security Profile is blocking the content, they only generate entries if the traffic is first allowed by a security rule and then subsequently flagged. Starting with the Traffic Log ensures the analyst doesn't miss "quiet" drops caused by simple policy mismatches or routing issues before moving on to deeper inspection logs.

Question 5. (Multi Select)

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

Correct Answer: C, D

Explanation:

Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:

In the Palo Alto Networks ecosystem, specifically when utilizing Strata Cloud Manager (SCM) and

Enterprise Data Loss Prevention (DLP), Data Filtering profiles are used to identify and protect sensitive information. When an analyst creates a custom data pattern to be used within these profiles, the system allows for two primary methods of identification: Regular Expressions (Regex) and File Properties.
Regular Expressions (D) allow the analyst to define a specific string or numerical pattern, such as a custom employee ID format or a proprietary project code. This is the most flexible and common way to catch sensitive text data within a file or data stream.
File Properties (C) allow the analyst to create patterns based on the metadata or attributes of a file rather than its contents. This includes identifying files based on the "Author," "Title," "Company," or even custom tags embedded in document properties (e.g., Microsoft Word or PDF metadata). By combining these two pattern types, a Network Security Analyst can create a highly granular detection engine. For instance, a policy could block any file where the "Company" property is set to a competitor or any file containing text that matches a specific Regex-defined sensitive data format.
While "Predefined" patterns (like Credit Card numbers) are also a core component, they are not listed as an option here. "Proximity Patterns" are a feature used to reduce false positives by ensuring two patterns appear near each other, but the fundamental "pattern types" for custom definitions are Regex and File Properties.