KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **NetSec Analyst**

Title : Palo Alto Networks Network Security Analyst

Version : DEMO

1.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."
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.

2.What is the most granular method for ensuring that traffic to a firewall’s public IP address on the public interface is translated to the private IP address of the web server?
A. Create one NAT policy, ensure the policy has original packet destination IP as the public IP address and translated packet destination IP as the private IP address, and mark Bi-directional as "Yes."
B. Create one NAT policy, set the source address to the public IP address and destination address to the private IP address, and ensure Bi-directional is checked.
C. Create two static NAT policies, ensure one policy has original packet destination IP as the public IP address and translated packet destination IP as the private IP address, ensure the other policy has original packet source IP as the private IP address and the translated packet source IP as the public IP address.
D. Create one NAT policy, ensure the policy has original packet source IP as the private IP address and the translated packet source IP as the public IP address, and mark Bi-directional as "Yes."
Answer: D
Explanation:
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
In Palo Alto Networks PAN-OS, the most efficient and granular way to configure a 1-to-1 static NAT

(Network Address Translation) for a server—such as a web server—is to use a Bi-directional NAT statement. The specific logic required by the firewall is to define the rule from the perspective of the outbound traffic (Source NAT) while enabling the "Bi-directional" checkbox.
When you create a NAT policy where the Original Packet source is the private IP address of the web server and the Translated Packet source is the public IP address, checking the Bi-directional box causes the firewall to automatically create an implicit "twin" rule. This hidden rule handles the inbound (Destination NAT) traffic, mapping the public IP back to the private IP for incoming requests.
Option D is correct because it correctly identifies the required "Original Source" as the private IP.
Option A is incorrect because Bi-directional NAT cannot be enabled on a rule where the translation type is Destination NAT.
Option C is technically functional but is not the most "granular" or efficient method, as it requires manual management of two separate rules, increasing the risk of configuration drift. By using the Bi-directional setting on the source-based rule, the analyst ensures that the server can both initiate outbound connections (like updates) and receive inbound traffic (like web requests) using a single, consistent mapping.

3.A financial company is deploying NGFWs with the Advanced SD-WAN subscription to improve uptime and bandwidth across thousands of ATMs. The company requires that traffic flows to the internal application needed by the ATMs always use the path with the lowest latency and packet loss.
Which unique SD-WAN rule parameters meet this criteria?
A. Application/Service: "Internal Application for ATMs" → Path Selection: "Best Available Path" in Traffic Distribution Profile.
B. Application/Service: "Internal Application for ATMs" & "Management" in Path Quality Profile → Path Selection "Any."
C. Application/Service: "Internal Application for ATMs" → Path Selection "Weighted Distribution" in Traffic Distribution Profile.
D. Application/Service: "Internal Application for ATMs" & "ATM Path(Custom)" in Path Quality Profile → Path Selection "Any."
Answer: A
Explanation:
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
Palo Alto Networks SD-WAN implementation utilizes Traffic Distribution Profiles to define how the firewall selects the optimal path for specific applications. To meet the requirement of selecting the path with the lowest latency and packet loss, the analyst must configure an SD-WAN policy rule that maps the specific application (the internal ATM app) to a distribution profile set to "Best Available Path."
In this configuration, the firewall evaluates the real-time performance metrics of all available links (such as ISP1, ISP2, or LTE) based on a linked Path Quality Profile. The Path Quality Profile defines the specific thresholds for latency, jitter, and packet loss. When the "Best Available Path" selection is used, the firewall dynamically compares these metrics and steers the traffic to the interface that currently exhibits the highest quality relative to those thresholds.
Option C is incorrect because Weighted Distribution is used for load sharing across multiple links based on a percentage, rather than selecting a single "best" path. Options B and D are incorrect because "Path Selection" logic is defined within the Traffic Distribution Profile, not the Path Quality Profile, and "Path

Selection: Any" would not prioritize performance metrics. By choosing "Best Available Path," the Network Security Analyst ensures high availability and optimal performance for mission-critical financial transactions, which is a key objective in modern distributed enterprise environments.

4.Which aspect of a network’s current health does the Strata Cloud Manager (SCM) Device Health dashboard provide?
A. Health trends based on which CVEs are not remediated.
B. Health score based on current physical hardware issues detected.
C. Health score based on security profile feature adoption.
D. Health trends for firewalls filtered by how long the issue has been experienced.
Answer: D
Explanation:
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
In a Palo Alto Networks environment, Strata Cloud Manager (SCM) serves as a centralized, AI-powered management platform that provides deep operational insights. The Device Health dashboard specifically focuses on the operational stability and performance of managed firewalls. Unlike security-focused dashboards that track threats or feature adoption, the Device Health dashboard is designed to help analysts identify and prioritize systemic operational issues.
+1
The core capability of this dashboard is providing health trends that allow administrators to see how performance anomalies—such as high CPU utilization, memory exhaustion, or packet buffer spikes—are behaving over time. Crucially, it allows analysts to filter these trends by the duration of the issue (e.g., issues persisting for 7 days, 30 days, or longer). This helps distinguish between a temporary "spike" in resource usage and a persistent configuration or capacity problem that requires remediation. By focusing on the duration and persistence of health issues, the Network Security Analyst can effectively perform root cause analysis and capacity planning. For instance, a firewall showing a high health impact for over 30 days indicates a chronic problem that might lead to a network outage, whereas a 1-day issue might be an isolated incident. This proactive monitoring aligns with the AIOps (Artificial Intelligence for IT Operations) strategy, moving the security team from a reactive "break-fix" model to a predictive maintenance model.

5.To comply with new regulations, a company requires all traffic logs related to the "HR-App" application across all Security policies be sent to a compliance syslog server. A Log Forwarding profile already exists to send logs to a default syslog server.
What is the most efficient process for configuring an NGFW to comply with the new regulations without disrupting existing traffic logs being sent to the default syslog server?
A. Edit the existing Log Forwarding profile by adding a new match list consisting of Log Forwarding filter for the application named "HR-App" to direct logs to the compliance syslog server.
B. Create a new Log Forwarding profile, update the profile with the details of the compliance syslog server and attach the profile to the relevant Security policy rule.
C. Edit the existing Log Forwarding profile, add a new entry, use the filter builder to match on application "HR-App," and add the details for the compliance syslog server.
D. Create a Log Forwarding profile and enable the predefined filter for "Application" In the associated

dropdown, select or create a new application object with the name "HR-App," and add the details for the compliance syslog server.

Answer: C

Explanation:

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

In Palo Alto Networks PAN-OS, Log Forwarding profiles are designed to be modular and scalable. To meet a specific compliance requirement—such as forwarding logs for a specific application like "HR-App" to a dedicated compliance server—the most efficient method is to modify the existing profile assigned to your security rules rather than creating new profiles and re-assigning them across the entire policy set. By editing the existing Log Forwarding profile and adding a new match list entry, an analyst can use the Filter Builder to create a specific query (e.g., (app eq 'HR-App')). Within this specific entry, you define the destination as the compliance syslog server. Because this is an additional entry within the same profile, it does not interfere with the default settings that send all other traffic logs to the standard syslog server.

This approach is considered "most efficient" because Log Forwarding profiles are typically applied to many security rules simultaneously. Updating the profile once ensures that any rule using that profile will now selectively branch "HR-App" logs to the compliance server, regardless of which security rule triggered the log. This minimizes administrative overhead and ensures consistent compliance across the entire security policy infrastructure without requiring a manual audit of every individual rule.