Vendor: Palo Alto Networks

Exam Code: NetSec-Analyst

Exam Name: Palo Alto Networks Network Security Analyst

Version: DEMO

QUESTION 1
What is the expected behavior of an NGFW for handling traffic that does not match any of the SD-WAN rules in the policy?

A. It will send the traffic out the first interface listed in the SD-WAN interface profile.
B. It will send the traffic using an implied SD-WAN round-robin rule.
C. It will not use SD-WAN but will fall back to the standard routing table to determine how to handle the traffic.
D. It will drop the traffic using an implied SD-WAN default deny rule.

Answer: C
Explanation:
If traffic does not match any SD-WAN policy rule, the firewall does not apply SD-WAN path selection and instead processes the traffic using the normal routing table, forwarding it according to standard routing behavior.

QUESTION 2
What is the most likely reason a primary data center firewall is no longer visible in the Strata Cloud Manager (SCM) dashboard?

A. Its environment is too complicated and cannot be onboarded in SCM.
B. Its firewall license has expired.
C. It does not have the appropriate device-level telemetry settings enabled.
D. User does not have the appropriate permissions.

Answer: C
Explanation:
Strata Cloud Manager relies on device-level telemetry to receive status, health, and visibility data from managed firewalls. If telemetry is not enabled or properly configured, the firewall cannot send information to SCM, causing it to be absent from the dashboard even though it may still be operational.

QUESTION 3
Beyond being a SaaS-based delivery platform, what is an advantage of Strata Cloud Manager (SCM) over Panorama?

A. Live, inline best practice checks
B. NGFW and Prisma Access management
C. Customizable dashboards
D. Real-time alerting

Answer: A
Explanation:
Strata Cloud Manager provides live, inline best practice checks that continuously evaluate configurations against Palo Alto Networks recommendations and immediately highlight risks or misconfigurations, offering proactive guidance that is not available in Panorama.

QUESTION 4
What is an important consideration when defining custom data patterns for data loss prevention (DLP) on Palo Alto Networks platforms?

A. They should be specific and tested to minimize false positives and false negatives.
B. They do not require regular updates once deployed.
C. They should be as broad as possible to cover all potential data types.
D. They are less effective than predefined patterns and should be avoided.

Answer: A
Explanation:
Custom data patterns must be carefully defined and validated so they accurately match only the intended sensitive data. Specific, well-tested patterns reduce false positives that disrupt users and false negatives that allow data leakage, ensuring effective and reliable DLP enforcement.

QUESTION 5
A team of analysts uses four NGWFs with the Precision AI Bundle, SaaS Security Inline, and Strata Cloud Manager Pro Collectively this secures all company assets across the data center and two remote sites. A security incident requires the team to review a mobile user, John Doe.

During the audit, the team prompts, "How was the application experience for John Doe over the past 60 days?"

What is an expected response from Strata Copilot?

A. "The average application test score for 'john doe' over the past 60 days is 37 67."
B. The user 'John Doe' encountered a total of 219 threats in the last 3 hours."
C. The top three threats impacting John Doe are phishing, SQL injections, and ransomware."
D. "Your organization doesn't have ADEM."

Answer: D
Explanation:
Application experience metrics are provided through Autonomous Digital Experience Management (ADEM). If ADEM is not licensed or deployed, Strata Copilot cannot generate user experience analytics and will indicate that the organization does not have ADEM available.

QUESTION 6
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: A
Explanation:
A destination NAT rule that maps the public IP as the original destination and translates it to the private server IP provides precise control over inbound traffic. Enabling bi-directional ensures

consistent return traffic handling while maintaining a single, granular NAT policy specifically for that public-to-private translation.

QUESTION 7
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: BD
Explanation:
Proximity patterns detect sensitive data by identifying keywords that appear near each other within a defined distance, improving contextual accuracy. Regular expressions match specific text formats or structured data patterns, enabling precise detection of sensitive information such as account numbers or identifiers.

QUESTION 8
A security manager asks for automated guidance on several OS security advisories released by Palo Alto Networks. Which steps can be taken on Strata Cloud Manager (SCM) to respond to the request?

A. Insights → Activity Insights → Threats, add a filter for threat category, review the logs, generate a weekly report.
B. Dashboard → PAN-OS CVEs, select the CVEs to review, generate upgrade recommendations.
C. Insights → Application Experience → Application Domains, add a filter for usage source, generate a weekly report.
D. Dashboard → Security Posture Insights, set time range to past 90 days, look at regressing scores in particular, generate a weekly report.

Answer: B
Explanation:
The PAN-OS CVEs section in Strata Cloud Manager provides direct visibility into operating system security advisories and vulnerabilities affecting managed firewalls, along with automated guidance and recommended software upgrades to remediate the identified risks.

QUESTION 9
Which CLI command will provide an overview of the CPU resources consumed by the data plane of a Palo Alto Networks firewall?

A. show system state
B. show system resources
C. show running resource-monitor
D. show running statistics

Answer: C
Explanation:
The resource monitor command displays real-time utilization for the data plane, including CPU consumption by packet processing and related processes. This provides a clear overview of how data plane resources are being used and helps diagnose performance issues.

QUESTION 10
A malware incident involving compromised internal hosts communicating with a command-and-control (C2) server has been resolved. In response, the C2 IP address is blocked. Which two actions using the Log Viewer will ensure the incident has been fully mitigated? (Choose two.)

A. Build and save a custom filter based on the affected endpoints and continue to monitor for suspicious traffic from the endpoints.
B. Review the authentication alerts on the affected devices.
C. Review the audit alerts and check for integrity protection alerts on the affected devices.
D. Continue to monitor for traffic going to the C2 server's IP address.

Answer: AD
Explanation:
Creating and saving a custom filter for the affected endpoints allows continuous monitoring of their activity to detect any remaining or recurring suspicious communications. Monitoring traffic to the blocked C2 IP verifies that no further connections are attempted, confirming that the malicious communication channel has been effectively contained.

QUESTION 11
What is the order of processing when both Policy Based Forwarding (PBF) policies and routing table entries are involved?

A. The firewall evaluates the routing table that is using the longest prefix match and then applies any matching PBF rule to override the next-hop.
B. The firewall evaluates PBF policies first; if a packet matches a PBF rule, the specified next-hop in that rule overrides the routing table.
C. The firewall performs a simultaneous evaluation of both PBF policies and the routing table, and then it chooses the route with the lowest metric.
D. The firewall evaluates static routes, then dynamic routes, and then it applies PBF policies to adjust the next-hop.

Answer: B
Explanation:
Policy Based Forwarding is evaluated before the routing table. If traffic matches a PBF rule, the firewall uses the next-hop defined in that rule and bypasses normal routing decisions, only consulting the routing table when no PBF rule matches.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**