PrepAwayPDF

ONLINE TEST ENGINE

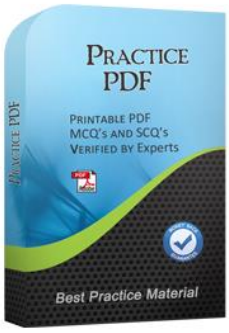
- Online Tool, Convenient, easy to study.
- Practice Online Anytime
- Instant Online Access
- Test History and Performance Review
- Supports All Web Browsers
- Supports Windows / Mac / Android / iOS, etc.

Online Test Engine

DESKTOP TEST ENGINE

- Installable Software Application
- Supports MS Operating System
- Simulates Real Exam Environment
- Two Modes For Practice
- Builds Exam Confidence
- Practice Offline Anytime

Desktop Test Engine



PDF PRACTICE Q&A'S

- Printable PDF Format
- Study Anywhere, Anytime
- Prepared by IT Experts
- 365 Days Free Updates
- Instant Access to Download
- Free PDF Demo Available

PDF Practice Q&A's

60920	59520	59062	59146
Demo Downloads	Successfull Cases	Satisfied Clients	The number of consulting

http://www.prepawaypdf.com/

Best Professional Test Guide Help You Pass and Provide Safe Shopping

Exam : **NetSec-Analyst**

Title : Palo Alto Networks Network Security Analyst

Vendor : Palo Alto Networks

Version : DEMO

NO.1 DNS rewrite can only be configured on a NAT rule with which type of destination address translation?

A. Dynamic IP and Port (DIPP)

B. Dynamic IP (with session distribution)

C. Static IP

D. Dynamic IP

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, the DNS rewrite feature (often referred to as DNS Doctoring) is specifically designed to solve the issue of split-horizon DNS in environments where internal users must access an internal server using its public IP address. This occurs when the DNS server returns the public IP address of a server to an internal client, but the client and server are on the same or related internal networks.

The firewall can only perform a DNS rewrite when a Static IP destination NAT rule is in place. When this option is enabled, the firewall monitors DNS responses passing through it. If a DNS response contains an IP address that matches the "Original Destination" IP in a static NAT rule, the firewall rewrites the DNS payload to the "Translated Destination" IP (the private IP of the server).

This functionality is restricted to Static IP translation because it requires a 1-to-1, predictable mapping between the public and private addresses. Dynamic translation types (A, B, and D) involve pools of addresses or port-overloading, which makes it impossible for the firewall to determine which specific internal IP address should be written into the DNS response at any given time. By ensuring a static mapping, the Network Security Analyst guarantees that internal clients receive the correct internal IP address to reach their destination without hair-pinning traffic unnecessarily through the public interface.

NO.2 An analyst needs to prevent users from downloading executable files from "High-Risk" URL categories while allowing them from "Business-and-Economy." Which profile should be configured to achieve this specific file-type restriction?

A. URL Filtering Profile

B. Data Filtering Profile

C. File Blocking Profile

D. Vulnerability Protection Profile

Answer: C

Explanation:

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

The File Blocking Profile is the primary tool used by Palo Alto Networks firewalls to control the movement of specific file types across the network. While a URL Filtering Profile (Option A) can block access to a website based on its category, it does not have the granular ability to distinguish between a PDF download and an EXE download on that site.

To meet the requirement, the analyst creates a File Blocking Profile with rules that target the .exe file extension. The profile allows the analyst to set actions like alert, block, or continue based on the direction of the traffic (upload or download) and the application being used. By attaching this profile

to a Security policy rule, the firewall uses Content-ID to look deep into the payload-beyond just the file extension-to identify the true file type. This prevents users from bypassing security by simply renaming a malicious .exe file to .txt.
This is a core objective for ensuring that sanctioned web browsing does not become a vector for malware delivery.

NO.3 In a Zero Trust environment, why is it recommended to use "User-ID" instead of just IP addresses in Security policy rules?

A. To allow the firewall to perform hardware-level decryption.

B. IP addresses are dynamic and do not provide persistent identity in modern networks.

C. User-ID is required to enable the "application-default" service setting.

D. Using User-ID reduces the CPU load on the Management Plane.

Answer: B

Explanation:
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
The transition from IP-based rules to identity-based rules is a cornerstone of the Network Security Analyst role. In modern environments-especially those with Wi-Fi, DHCP, and remote workers-an IP address is a temporary identifier that can change multiple times a day. Relying solely on IPs makes it difficult to maintain accurate security audits and granular control.
By implementing User-ID, the analyst maps IP addresses to specific users and groups retrieved from an identity provider like Active Directory or Okta. This allows the analyst to write rules like "Allow HR-Group to access HR-SaaS-App," which remains effective regardless of which IP address the HR employee is currently using. This provides persistent visibility and control, ensuring that security policies follow the user rather than the device. This is a critical objective for achieving a Zero Trust architecture, where identity is verified at every step of the communication process.

NO.4 An analyst needs to configure a NAT policy to allow internal users to access the internet. The company only has one public IP address available on the firewall's outside interface. Which NAT type should be used?

A. Static IP

B. Dynamic IP

C. Dynamic IP and Port (DIPP)

D. Bi-directional NAT

Answer: C

Explanation:
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
In environments with limited public IP addresses, Dynamic IP and Port (DIPP) NAT-also known as Port Address Translation (PAT)-is the standard solution for outbound internet access.
DIPP allows the firewall to translate multiple internal private IP addresses to a single public IP address by assigning a unique source port to each internal session. The firewall maintains a translation table to ensure that returning traffic from the internet is routed back to the correct internal host. This is the most efficient way to provide internet connectivity for a large number of users using a minimal amount of public IP space. For an analyst, configuring DIPP is a core task that involves defining a

"Source NAT" rule where the "Original Packet" is the internal subnet and the "Translated Packet" uses the interface address of the firewall's public- facing port.

NO.5 An analyst notices latency on the firewall and wants to improve performance. Which steps can be taken to reduce management plane CPU while working to determine the underlying problem?

A. Disable log at session start and only log at session end.

B. Enable log forwarding from the firewall to an external destination.

C. Enable logging for intrazone-default and interzone-default security rules.

D. Disable log at session end and only log at session start.

Answer: A

NO.6 What is an important consideration when defining custom data patterns for data loss prevention (DLP) on Palo Alto Networks platforms? (Choose one answer)

A. They do not require regular updates once deployed.

B. They are less effective than predefined patterns and should be avoided.

C. They should be specific and tested to minimize false positives and false negatives.

D. They should be as broad as possible to cover all potential data types.

Answer: C

Explanation:

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

Custom data patterns allow organizations to extend the capabilities of Data Loss Prevention (DLP) beyond standard identifiers (like Credit Card numbers or SSNs) to include proprietary data such as internal project codes, intellectual property, or specialized legal documents. Because these patterns are typically defined using Regular Expressions (Regex), the most critical administrative consideration is ensuring they are specific and thoroughly tested.

If a custom pattern is defined too broadly (Option D), it will trigger a high volume of false positives, where legitimate, non-sensitive traffic is flagged or blocked. This "noise" creates alert fatigue for the security team and can disrupt business operations. Conversely, a pattern that is not specific enough can result in false negatives, allowing sensitive data to exit the network undetected. A Network Security Analyst must test these patterns against a variety of sample data sets to confirm they correctly identify the intended information across different file formats and protocols. This iterative testing and refinement process is essential for maintaining the accuracy and reliability of the DLP solution, ensuring that protection is both effective and non-disruptive to the flow of valid business information.

NO.7 An organization needs to implement a security rule that allows users to access "Facebook" but prevents them from using "Facebook-Chat." What is the best way to achieve this?

A. Create a URL Filtering profile to block the chat URL.

B. Create a security rule allowing the "Facebook-base" App-ID and another rule blocking the "Facebook- chat" App-ID.

C. Use an Application Override rule for Facebook traffic.

D. Block the specific IP addresses used by Facebook Chat.

Answer: B

Explanation:

Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
The power of App-ID lies in its ability to distinguish between different functions within the same web service. Palo Alto Networks provides specific App-IDs for various sub-functions of popular sites.
To achieve the requirement, the analyst should create two security rules (or one rule with a specific exclusion). The first rule, placed higher in the policy, would block the Facebook-chat App-ID. The second rule, placed below it, would allow the Facebook-base App-ID. Because the firewall evaluates rules from the top down, any attempt to use the chat function will hit the block rule first. This provides much higher security and granularity than URL Filtering (Option A), which might struggle to differentiate between the different elements of a dynamic, HTTPS-based site like Facebook. Using App-ID for this purpose ensures that the business can allow the useful parts of social media while mitigating the risks associated with unauthorized file transfers or interactive chat functions.

NO.8 A company requires that all file transfers only over HTTP (tcp/80 and tcp/8080) to SaaS storage must be inspected for data exfiltration. Traffic to encrypted HTTPS SaaS storage cannot be inspected based on the company decryption restrictions.
When using a security profile group, which Security policy configuration meets this requirement?
A. One with data filtering to inspect all HTTP traffic on the web-browsing application using application- default for the service.
B. One with URL filtering and file blocking to block all file uploads to the URL category online-storage-and-backup, then set the service to tcp/80 and tcp/8080.
C. One with data filtering and the service set to tcp/80 and tcp/8080, then verify block threshold is set to
"1" to stop exfiltration.
D. One with data filtering and an application filter that matches "file-sharing" applications, then set the service to tcp/80 and tcp/8080.
Answer: D
Explanation:
Comprehensive and Detailed 150 to 250 words of Explanation From Palo Alto Networks Network Security Analyst Knowledge:
To address data exfiltration specifically for SaaS and file-sharing platforms over non-encrypted channels, a Network Security Analyst must combine the power of App-ID with Data Filtering Profiles. The requirement specifies that inspection must occur over specific ports (tcp/80 and tcp/8080) and target SaaS storage.
Option D is the most accurate because it utilizes an Application Filter. Application filters are dynamic objects that automatically include applications sharing specific characteristics-in this case, the "file-sharing" subcategory which encompasses SaaS storage providers. By setting the Service to a custom service object containing ports tcp/80 and tcp/8080, the analyst ensures the rule only triggers on the unencrypted traffic specified in the requirement.
The Data Filtering Profile is the specific security profile designed to detect patterns (like credit card numbers, Social Security numbers, or custom regex) within file transfers to prevent exfiltration. While Option C mentions data filtering and the correct ports, it lacks the application specificity (SaaS storage) required.
Option A is too broad as it only targets "web-browsing," which may not capture specific file-sharing App-IDs.
By using an application filter, the analyst ensures that as new SaaS storage applications emerge, they

are automatically added to the inspection policy, maintaining a robust security posture against data leakage.