Download Palo Alto Networks NetSec-Pro Exam Dumps Free

Shared by Vasquez on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How does a firewall behave when SSL Inbound Inspection is enabled?

Options:

A- It acts transparently between the client and the internal server.
B- It decrypts inbound and outbound SSH connections.
C- It decrypts traffic between the client and the external server.
D- It acts as meddler-in-the-middle between the client and the internal server.

Answer:

D

Explanation:

SSL Inbound Inspection allows the firewall to decrypt incoming encrypted traffic to internal servers (e.g., web servers) by acting as a man-in-the-middle (MITM). The firewall uses the private key of the server to decrypt the session and apply security policies before re-encrypting the traffic.

''SSL Inbound Inspection requires you to import the server's private key and certificate into the firewall. The firewall then acts as a man-in-the-middle (MITM) to decrypt inbound sessions from external clients to internal servers for inspection.''

(Source: SSL Inbound Inspection)

Question 2

Question Type: MultipleChoice

Which offering can be managed in both Panorama and Strata Cloud Manager (SCM)?

Options:

A- Autonomous Digital Experience Manager (ADEM)
B- VM-Series Next-Generation Firewall (NGFW)

C- Prisma SD-WAN
D- SaaS Security

Answer:

B

Explanation:

The VM-Series NGFWs are designed to integrate seamlessly with both Panorama and Strata Cloud Manager (SCM), allowing administrators to manage physical and virtual firewall deployments from either interface.

''You can manage VM-Series Next-Generation Firewalls using either Panorama for centralized management of all firewalls or Strata Cloud Manager for cloud-based management, giving flexibility across hybrid environments.''

(Source: VM-Series Management Options)

Unified management flexibility is key for enterprises with hybrid or multi-cloud deployments.

Question 3

Question Type: MultipleChoice

Which component of NGFW is supported in active/passive design but not in active/active design?

Options:

A- Single floating IP address
B- Using a DHCP client
C- Route-based redundancy
D- Configuring ARP load-sharing on Layer 3

Answer:

A

Explanation:

Single floating IP address (also known as a floating IP or shared IP) is supported only in an

active/passive HA pair. In active/active HA, both firewalls are forwarding traffic simultaneously and thus do not share a single floating IP.

''In active/passive HA, a single floating IP address is used for seamless failover. Active/active HA requires separate IP addresses and does not support a single floating IP.''

(Source: Active/Passive vs. Active/Active HA)

This simplifies failover in active/passive deployments by using a single shared IP that moves to the active peer upon failover.

Question 4

Question Type: MultipleChoice

During a security incident investigation, which Security profile will have logs of attempted confidential data exfiltration?

Options:

A- File Blocking Profile
B- Enterprise DLP Profile
C- Vulnerability Protection Profile
D- WildFire Analysis Profile

Answer:

B

Explanation:

Enterprise DLP Profile is specifically designed to detect and log data exfiltration attempts, including those involving confidential or sensitive data.

''Enterprise DLP logs capture incidents involving potential data exfiltration. They help identify sensitive data transfers, even in seemingly legitimate traffic.''

(Source: Enterprise DLP Logging and Alerts)

File Blocking and Vulnerability Protection handle files or exploit detection, while WildFire focuses on malware analysis---not direct data exfiltration.

Question 5

Question Type: MultipleChoice

Which method in the WildFire analysis report detonates unknown submissions to provide visibility into real-world effects and behavior?

Options:

A- Dynamic analysis
B- Static analysis
C- Intelligent Run-time Memory Analysis
D- Machine learning (ML)

Answer:

A

Explanation:

Dynamic analysis in WildFire refers to executing unknown files in a controlled environment (sandbox) to observe their real-world behavior. This allows the firewall to detect zero-day threats and advanced malware by directly analyzing the file's impact on a system.

''WildFire dynamic analysis detonates unknown files in a secure sandbox environment, analyzing real-world effects, behaviors, and potential malicious activity.''

(Source: WildFire Analysis)

Question 6

Question Type: MultipleChoice

What is a necessary step for creation of a custom Prisma Access report on Strata Cloud Manager (SCM)?

Options:

A- Open a support ticket.
B- Set up Cloud Identity Engine.
C- Generate a PDF summary report.
D- Configure a dashboard.

Answer:

D

Explanation:

To create custom Prisma Access reports within SCM, you first configure a dashboard that aggregates the relevant logs and analytics. This allows you to define the data points you want to include.

''Dashboards in SCM can be customized to include Prisma Access data sources, enabling you to create and generate reports that meet specific business and security requirements.''

(Source: SCM Dashboards and Reporting)

Once configured, you can export the dashboard as a custom report.

''Use the dashboard's data visualization to create custom reports for Prisma Access, which can be exported as PDFs for distribution.''

(Source: SCM Report Customization)