



PSE-STRATA^{Q&As}

Palo Alto Networks System Engineer Professional-Strata

Pass PSE-STRATA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/pse-strata.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Official
Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

Which two network events are highlighted through correlation objects as potential security risks? (Choose two.)

- A. Identified vulnerability exploits
- B. Launch of an identified malware executable file
- C. Endpoints access files from a removable drive
- D. Suspicious host behavior

Correct Answer: AD

QUESTION 2

What will best enhance security of a production online system while minimizing the impact for the existing network?

- A. Layer 2 interfaces
- B. active / active high availability (HA)
- C. Virtual wire
- D. virtual systems

Correct Answer: C

QUESTION 3

Which two email links, contained in SMTP and POP3, can be submitted from WildFire analysis with a WildFire subscription? (Choose two.)

- A. FTP
- B. HTTPS
- C. RTP
- D. HTTP

Correct Answer: BD

QUESTION 4

Which functionality is available to firewall users with an active Threat Prevention subscription, but no WildFire license?

- A. WildFire hybrid deployment



- B. 5 minute WildFire updates to threat signatures
- C. Access to the WildFire API
- D. PE file upload to WildFire

Correct Answer: D

QUESTION 5

Which two steps are required to configure the Decryption Broker? (Choose two.)

- A. reboot the firewall to activate the license
- B. activate the Decryption Broker license
- C. enable SSL Forward Proxy decryption
- D. enable a pair of virtual wire interfaces to forward decrypted traffic

Correct Answer: BD

QUESTION 6

A service provider has acquired a pair of PA-7080s for its data center to secure its customer base's traffic. The server provider's traffic is largely generated by smart phones and averages 6,000,000 concurrent sessions.

Which Network Processing Card should be recommended in the Bill of Materials?

- A. PA-7000-20GQ-NPC
- B. PA-7000-40G-NPC
- C. PA-7000-20GQXM-NPC
- D. PA-7000-20G-NPC

Correct Answer: C

QUESTION 7

A customer requires protections and verdicts for portable executable (PE) and executable and linkable format (ELF), as well as the ability to integrate with existing security tools.

Which Cloud-Delivered Security Service (CDSS) does Palo Alto Networks provide that will address this requirement?

- A. Dynamic Unpacking
- B. WildFire
- C. DNS Security



D. File Blocking profile

Correct Answer: B

QUESTION 8

A customer is looking for an analytics tool that uses the logs on the firewall to detect actionable events on the network. They require something to automatically process a series of related threat events that, when combined, indicate a likely compromised host on their network or some other higher level conclusion. They need to pinpoint the area of risk, such as compromised hosts on the network, allows you to assess the risk and take action to prevent exploitation of network resources.

Which feature of PAN-OS can you talk about to address their requirement to optimize their business outcomes?

- A. The Automated Correlation Engine
- B. Cortex XDR and Cortex Data Lake
- C. WildFire with API calls for automation
- D. 3rd Party SIEM which can ingest NGFW logs and perform event correlation

Correct Answer: A

Reference: <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/monitoring/use-the-automated-correlation-engine.html>

QUESTION 9

Which filtering criterion is used to determine users to be included as members of a dynamic user group (DUG)?

- A. Security policy rule
- B. Tag
- C. Login ID
- D. IP address

Correct Answer: B

QUESTION 10

When HTTP header logging is enabled on a URL Filtering profile, which attribute-value can be logged?

- A. X-Forwarded-For
- B. HTTP method
- C. HTTP response status code



D. Content type

Correct Answer: A

QUESTION 11

What are two ways to manually add and remove members of dynamic user groups (DUGs)? (Choose two)

- A. Add the user to an external dynamic list (EDL).
- B. Tag the user using Panorama or the Web UI of the firewall.
- C. Tag the user through the firewalls XML API.
- D. Tag the user through Active Directory

Correct Answer: BC

QUESTION 12

In which two cases should the Hardware offering of Panorama be chosen over the Virtual Offering? (Choose two.)

- A. Dedicated Logger Mode is required
- B. Logs per second exceed 10,000
- C. Appliance needs to be moved into data center
- D. Device count is under 100

Correct Answer: AB

QUESTION 13

Which proprietary technology solutions will allow a customer to identify and control traffic sources regardless of internet protocol (IP) address or network segment?

- A. User ID and Device-ID
- B. Source-D and Network.ID
- C. Source ID and Device-ID
- D. User-ID and Source-ID

Correct Answer: A

QUESTION 14



What are two benefits of the sinkhole Internet Protocol (IP) address that DNS Security sends to the client in place of malicious IP addresses? (Choose two.)

- A. The client communicates with it instead of the malicious IP address
- B. It represents the remediation server that the client should visit for patching
- C. It will take over as the new DNS resolver for that client and prevent further DNS requests from occurring in the meantime
- D. In situations where the internal DNS server is between the client and the firewall, it gives the firewall the ability to identify the clients who originated the query to the malicious domain

Correct Answer: AD

QUESTION 15

A prospective customer currently uses a firewall that provides only Layer 4 inspection and protections. The customer sees traffic going to an external destination, port 53, but cannot determine what Layer 7 application traffic is going over that port

Which capability of PAN-OS would address the customer's lack of visibility?

- A. Device ID, because it will give visibility into which devices are communicating with external destinations over port 53
- B. single pass architecture (SPA), because it will improve the performance of the Palo Alto Networks Layer 7 inspection
- C. User-ID, because it will allow the customer to see which users are sending traffic to external destinations over port 53
- D. App-ID, because it will give visibility into what exact applications are being run over that port and allow the customer to block unsanctioned applications using port 53

Correct Answer: D

[PSE-STRATA PDF Dumps](#)

[PSE-STRATA VCE Dumps](#)

[PSE-STRATA Study Guide](#)