

Paloalto Networks

PSE-PLATFORM Exam

PSE Platform Exam

**Questions & Answers
Demo**

Version: 9.0

Question: 1

Which two components must to be configured within User-ID on a new firewall that has been implemented? (Choose two.)

- A. Group Mapping
- B. 802.1X Authentication
- C. Proxy Authentication
- D. User mapping

Answer: AD

Explanation:

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/enable-user-id>

Question: 2

A specific URL keeps appearing in URL filtering log entries, it was blocked successfully, but the administrator would like to investigate further.

In which two ways would AutoFocus help this administrator? (Choose two.)

- A. Generate a list of IP addresses for use in Dynamic Address Groups on the firewall
- B. Identify malicious files associated with this URL
- C. Generate a correlation object that can be used to monitor associated activities
- D. Identify malware campaigns associated with this URL

Answer: AD

Question: 3

What are three sources of malware sample data for the Palo Alto Networks Threat Intelligence Cloud? (Choose three.)

- A. Third-Party data feeds, like the partnership with ProofPoint and the Cyber Threat Alliance
- B. Palo Alto Networks AutoFocus generated Correlation Objects
- C. Palo Alto Networks Next Generation Firewalls deployed with Wildfire Analysis Security Profiles
- D. WF-500 configured as private clouds for privacy concerns
- E. Palo Alto Networks non-firewall products, like Traps and Aperture

Answer: ABE

Explanation:

<https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/autofocus>

Question: 4

Which variable is used to regulate the rate of file submission to WildFire?

- A. Based on the purchase license
- B. Maximum number of files per minute
- C. Available bandwidth
- D. Maximum number of files per day

Answer: B

Explanation:

https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/submit-files-for-wildfire-analysis/firewall-file-forwarding-capacity-by-model

Question: 5

Which three items contain information about Command and Control (C&C) hosts? (Choose three.)

- A. Threat logs
- B. Data filtering logs
- C. Botnet reports
- D. SaaS reports
- E. WildFire analysts reports

Answer: BCE
