



PSE-PLATFORM^{Q&As}

PSE-Platform Professional

Pass Palo Alto Networks PSE-PLATFORM Exam with 100% Guarantee

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

<https://www.passapply.com/pse-platform.html>

100% Passing Guarantee
100% Money Back Assurance

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

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





QUESTION 1

The botnet report displays a confidence score of 1 to 5 indicating the likelihood of a botnet infection.

Which three sources are used by the firewall as the basis of this score? (Choose three.)

- A. Bad Certificate Reports
- B. Traffic Type
- C. Botnet Reports
- D. Number of Events
- E. Executable Downloads
- F. Threat Landscape

Correct Answer: BDE

Explanation: <https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/monitoring/generatebotnet-reports>

QUESTION 2

DNS sinkholing helps identify infected hosts on the protected network using DNS traffic in situations where the firewall cannot see the infected client's DNS query (that is, the firewall cannot see the originator of DNS query)

Which of the following Statements is true?

- A. DNS Sinkholing requires the Vulnerability Protection Profile be enabled.
- B. Sinkholing malware DNS queries solves this visibility problem by forging responses to the client host queries directed at fake domains created in a controlled "Fake Internet" called Zanadu which designed for testing and honeypots.
- C. Infected hosts can then be easily identified in the traffic logs because any host that attempts to connect the sinkhole IP address are most likely infected with malware.
- D. DNS Sinkholing requires a license SinkHole license in order to activate.

Correct Answer: C

QUESTION 3

Which three signature-based Threat Prevention features of the firewall are informed by intelligence from the Threat Intelligence Cloud? (Choose three.)

- A. Vulnerability protection
- B. Anti-Spyware



- C. Anti-Virus
- D. Botnet detection
- E. App-ID protection

Correct Answer: ABE

QUESTION 4

Which configuration creates the most comprehensive "best-practice" Anti Spyware profile to prevent command and Control traffic?

- A. Clone the Strict Anti-Spyware Profile, enable DNS Sinkholing and Passive DNS Monitoring, and deploy this customized clone
- B. Clone the Default Anti-Spyware Profile and enable DNS Sinkholing and Passive DNS Monitoring, and deploy this customized clone
- C. Edit and deploy the Default Anti-Spyware Profile (DNS Sinkholing and Passive DNS Monitoring is already enabled)
- D. Edit and deploy the Strict Anti-Spyware Profile Profile (DNS Sinkholing and Passive DNS Monitoring is already enabled)

Correct Answer: A

QUESTION 5

What is a best practice when configuring a security policy to completely block a specific application?

- A. On the Service/URL. Category tab, set the service to any
- B. On the Actions tab, configure a file blocking security profile
- C. On the Service/URL. Category tab, set the service to application-default
- D. On the Service/URL. Category tab, manually specify a port/service

Correct Answer: A

[PSE-PLATFORM Practice Test](#)

[PSE-PLATFORM Study Guide](#)

[PSE-PLATFORM Exam Questions](#)