



PCCET^{Q&As}

Palo Alto Networks Certified Cybersecurity Entry-level Technician

Pass Palo Alto Networks PCCET Exam with 100% Guarantee

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

<https://www.pass4itsure.com/pccet.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

In addition to local analysis, what can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware?

- A. Cortex XDR
- B. AutoFocus
- C. MineMild
- D. Cortex XSOAR

Correct Answer: A

In addition to local analysis, Cortex XDR can send unknown files to WildFire for discovery and deeper analysis to rapidly detect.

QUESTION 2

Which Palo Alto Networks subscription service complements App-ID by enabling you to configure the next- generation firewall to identify and control access to websites and to protect your organization from websites hosting malware and phishing pages?

- A. Threat Prevention
- B. DNS Security
- C. WildFire
- D. URL Filtering

Correct Answer: D

The URL Filtering service complements App-ID by enabling you to configure the next- generation firewall to identify and control access to websites and to protect your organization from websites that host malware and phishing pages.

QUESTION 3

Which network firewall operates up to Layer 4 (Transport layer) of the OSI model and maintains information about the communication sessions which have been established between hosts on trusted and untrusted networks?

- A. Group policy
- B. Stateless
- C. Stateful
- D. Static packet-filter

Correct Answer: C



Stateful packet inspection firewalls Second-generation stateful packet inspection (also known as dynamic packet filtering) firewalls have the following characteristics: They operate up to Layer 4 (Transport layer) of the OSI model and maintain state information about the communication sessions that have been established between hosts on the trusted and untrusted networks. They inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, and ICMP), and port number (during session establishment only) to determine whether the session should be allowed, blocked, or dropped based on configured firewall rules. After a permitted connection is established between two hosts, the firewall creates and deletes firewall rules for individual connections as needed, thus effectively creating a tunnel that allows traffic to flow between the two hosts without further inspection of individual packets during the session. This type of firewall is very fast, but it is port-based and it is highly dependent on the trustworthiness of the two hosts because individual packets aren't inspected after the connection is established.

QUESTION 4

What does SOAR technology use to automate and coordinate workflows?

- A. algorithms
- B. Cloud Access Security Broker
- C. Security Incident and Event Management
- D. playbooks

Correct Answer: D

SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.

QUESTION 5

Which tool supercharges security operations center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security?

- A. Prisma SAAS
- B. WildFire
- C. Cortex XDR
- D. Cortex XSOAR

Correct Answer: D

Cortex XSOAR enhances Security Operations Center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security. Cortex XSOAR unifies case management, automation, real-time collaboration, and native threat intel management in the industry's first extended security orchestration, automation, and response (SOAR) offering.