



# **Paloalto-Networks**

## **Exam Questions PCCET**

Palo Alto Networks Certified Cybersecurity Entry-level Technician

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

**NEW QUESTION 1**

Which type of Wi-Fi attack depends on the victim initiating the connection?

- A. Evil twin
- B. Jasager
- C. Parager
- D. Mirai

**Answer:** B

**NEW QUESTION 2**

Which term describes data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center?

- A. North-South traffic
- B. Intrazone traffic
- C. East-West traffic
- D. Interzone traffic

**Answer:** A

**NEW QUESTION 3**

Which organizational function is responsible for security automation and eventual vetting of the solution to help ensure consistency through machine-driven responses to security issues?

- A. NetOps
- B. SecOps
- C. SecDevOps
- D. DevOps

**Answer:** B

**NEW QUESTION 4**

DRAG DROP

Match the Identity and Access Management (IAM) security control with the appropriate definition.

IAM security		Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity		Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics		Securing and managing the relationships between users and cloud resources
Access Management		Decoupling workload identity from IP addresses

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

IAM security	IAM security	Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity	User Entity Behavior Analytics	Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics	Access Management	Securing and managing the relationships between users and cloud resources
Access Management	Machine Identity	Decoupling workload identity from IP addresses

#### NEW QUESTION 5

Which not-for-profit organization maintains the common vulnerability exposure catalog that is available through their public website?

- A. Department of Homeland Security
- B. MITRE
- C. Office of Cyber Security and Information Assurance
- D. Cybersecurity Vulnerability Research Center

**Answer:** B

#### NEW QUESTION 6

What is the primary security focus after consolidating data center hypervisor hosts within trust levels?

- A. control and protect inter-host traffic using routers configured to use the Border Gateway Protocol (BGP) dynamic routing protocol
- B. control and protect inter-host traffic by exporting all your traffic logs to a sysvol log server using the User Datagram Protocol (UDP)
- C. control and protect inter-host traffic by using IPv4 addressing
- D. control and protect inter-host traffic using physical network security appliances

**Answer:** D

#### NEW QUESTION 7

A native hypervisor runs:

- A. with extreme demands on network throughput
- B. only on certain platforms
- C. within an operating system's environment
- D. directly on the host computer's hardware

**Answer:** D

#### NEW QUESTION 8

Which Palo Alto Networks product provides playbooks with 300+ multivendor integrations that help solve any security use case?

- A. Cortex XSOAR
- B. Prisma Cloud
- C. AutoFocus
- D. Cortex XDR

**Answer:** A

#### NEW QUESTION 9

Which option would be an example of PII that you need to prevent from leaving your enterprise network?

- A. Credit card number
- B. Trade secret
- C. National security information
- D. A symmetric encryption key

**Answer:** A

#### NEW QUESTION 10

Systems that allow for accelerated incident response through the execution of standardized and automated playbooks that work upon inputs from security technology and other data flows are known as what?

- A. XDR
- B. STEP

- C. SOAR
- D. SIEM

**Answer:** C

**NEW QUESTION 10**

Which TCP/IP sub-protocol operates at the Layer7 of the OSI model?

- A. UDP
- B. MAC
- C. SNMP
- D. NFS

**Answer:** C

**NEW QUESTION 12**

Which IPsec feature allows device traffic to go directly to the Internet?

- A. Split tunneling
- B. Diffie-Hellman groups
- C. d.Authentication Header (AH)
- D. IKE Security Association

**Answer:** A

**NEW QUESTION 15**

Which Palo Alto subscription service identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment?

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

**Answer:** C

**NEW QUESTION 18**

In which step of the cyber-attack lifecycle do hackers embed intruder code within seemingly innocuous files?

- A. weaponization
- B. reconnaissance
- C. exploitation
- D. delivery

**Answer:** D

**NEW QUESTION 22**

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

**Answer:** D

**NEW QUESTION 27**

On an endpoint, which method is used to protect proprietary data stored on a laptop that has been stolen?

- A. operating system patches
- B. full-disk encryption
- C. periodic data backups
- D. endpoint-based firewall

**Answer:** B

**NEW QUESTION 31**

Why have software developers widely embraced the use of containers?

- A. Containers require separate development and production environments to promote authentic code.
- B. Containers share application dependencies with other containers and with their host computer.
- C. Containers simplify the building and deploying of cloud native applications.
- D. Containers are host specific and are not portable across different virtual machine hosts.

**Answer:** C

#### NEW QUESTION 34

When signature-based antivirus software detects malware, what three things does it do to provide protection? (Choose three.)

- A. decrypt the infected file using base64
- B. alert system administrators
- C. quarantine the infected file
- D. delete the infected file
- E. remove the infected file's extension

**Answer:** CDE

#### NEW QUESTION 36

What does Palo Alto Networks Cortex XDR do first when an endpoint is asked to run an executable?

- A. run a static analysis
- B. check its execution policy
- C. send the executable to WildFire
- D. run a dynamic analysis

**Answer:** B

#### NEW QUESTION 37

What is the key to “taking down” a botnet?

- A. prevent bots from communicating with the C2
- B. install openvas software on endpoints
- C. use LDAP as a directory service
- D. block Docker engine software on endpoints

**Answer:** A

#### NEW QUESTION 41

Which two network resources does a directory service database contain? (Choose two.)

- A. Services
- B. /etc/shadow files
- C. Users
- D. Terminal shell types on endpoints

**Answer:** AC

#### NEW QUESTION 46

.....

## Relate Links

**100% Pass Your PCCET Exam with Exambible Prep Materials**

<https://www.exambible.com/PCCET-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>