



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.passapply.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

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

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

Correct Answer: A

Perhaps the easiest way for an attacker to find a victim to exploit is to set up a wireless access point that serves as a bridge to a real network. An attacker can inevitably bait a few victims with "free Wi-Fi access." The main problem with this approach is that it requires a potential victim to stumble on the access point and connect. The attacker can't easily target a specific victim, because the attack depends on the victim initiating the connection.

<https://www.paloaltonetworks.com/blog/2013/11/wireless-man-middle/>

QUESTION 2

What is a key advantage and key risk in using a public cloud environment?

- A. Multi-tenancy
- B. Dedicated Networks
- C. Dedicated Hosts
- D. Multiplexing

Correct Answer: A

Multitenancy is a key characteristic of the public cloud, and an important risk. Although public cloud providers strive to ensure isolation between their various customers, the infrastructure and resources in the public cloud are shared. Inherent risks in a shared environment include misconfigurations, inadequate or ineffective processes and controls, and the "noisy neighbor" problem (excessive network traffic, disk I/O, or processor use can negatively impact other customers sharing the same resource). In hybrid and multicloud environments that connect numerous public and/or private clouds, the delineation becomes blurred, complexity increases, and security risks become more challenging to address.

QUESTION 3

Routing Information Protocol (RIP), uses what metric to determine how network traffic should flow?

- A. Shortest Path
- B. Hop Count
- C. Split Horizon



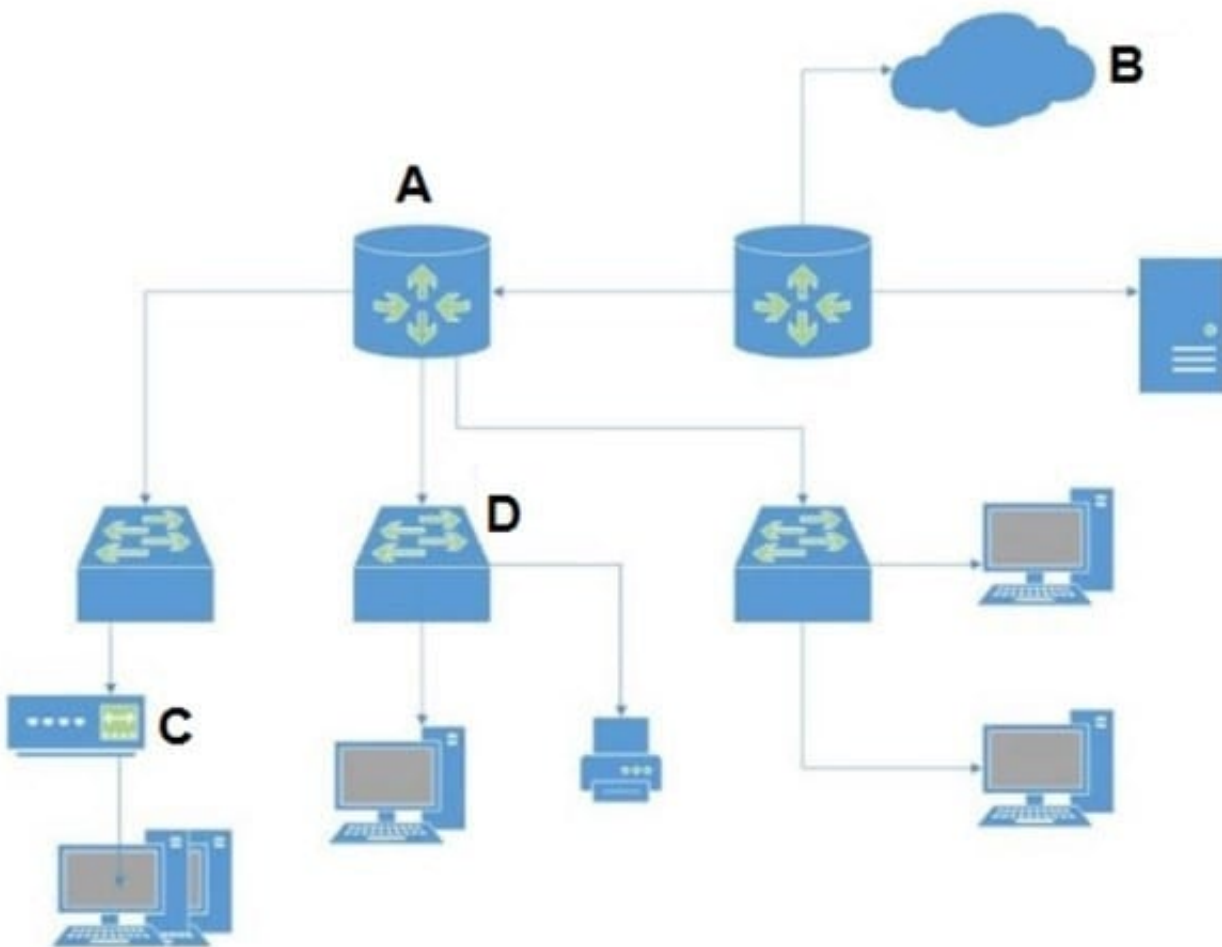
D. Path Vector

Correct Answer: B

Routing Information Protocol (RIP) is an example of a distance-vector routing protocol that uses hop count as its routing metric. To prevent routing loops, in which packets effectively get stuck bouncing between various router nodes, RIP implements a hop limit of 15, which limits the size of networks that RIP can support. After a data packet crosses 15 router nodes (hops) between a source and a destination, the destination is considered unreachable.

QUESTION 4

In the attached network diagram, which device is the switch?



A. A

B. B

C. C

D. D

Correct Answer: D



QUESTION 5

Which model would a customer choose if they want full control over the operating system(s) running on their cloud computing platform?

- A. SaaS
- B. DaaS
- C. PaaS
- D. IaaS

Correct Answer: D

QUESTION 6

Which attacker profile uses the internet to recruit members to an ideology, to train them, and to spread fear and include panic?

- A. cybercriminals
- B. state-affiliated groups
- C. hacktivists
- D. cyberterrorists

Correct Answer: D

QUESTION 7

Which element of the security operations process is concerned with using external functions to help achieve goals?

- A. interfaces
- B. business
- C. technology
- D. people

Correct Answer: A

The six pillars include:

1.
Business (goals and outcomes)
- 2.



People (who will perform the work)

3.

Interfaces (external functions to help achieve goals)

4.

Visibility (information needed to accomplish goals)

5.

Technology (capabilities needed to provide visibility and enable people)

6.

Processes (tactical steps required to execute on goals)

QUESTION 8

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

Correct Answer: C

"The WildFire cloud-based malware analysis environment is a cyber threat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment. WildFire automatically disseminates updated protections in near-real time to immediately prevent threats from spreading; this occurs without manual intervention"

QUESTION 9

Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) fall under which Prisma access service layer?

- A. Network
- B. Management
- C. Cloud
- D. Security

Correct Answer: D

A SASE solution converges networking and security services into one unified, cloud-delivered solution (see Figure 3-12)



that includes the following:

Networking

Software-defined wide-area networks (SD-WANs)

Virtual private networks (VPNs)

Zero Trust network access (ZTNA)

Quality of Service (QoS)

Security

Firewall as a service (FWaaS)

Domain Name System (DNS) security

Threat prevention

Secure web gateway (SWG)

Data loss prevention (DLP)

Cloud access security broker (CASB)

QUESTION 10

Which type of malware takes advantage of a vulnerability on an endpoint or server?

- A. technique
- B. patch
- C. vulnerability
- D. exploit

Correct Answer: A

QUESTION 11

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

Correct Answer: AC



A directory service is a database that contains information about users, resources, and services in a network.

QUESTION 12

Which IoT connectivity technology is provided by satellites?

- A. 4G/LTE
- B. VLF
- C. L-band
- D. 2G/2.5G

Correct Answer: C

2G/2.5G: 2G connectivity remains a prevalent and viable IoT connectivity option due to the low cost of 2G modules, relatively long battery life, and large installed base of 2G sensors and M2M applications.

3G: IoT devices with 3G modules use either Wideband Code Division Multiple Access (W-CDMA) or Evolved High Speed Packet Access (HSPA+ and Advanced HSPA+) to achieve data transfer rates of 384Kbps to 168Mbps. 4G/Long-Term

Evolution (LTE): 4G/LTE networks enable real-time IoT use cases, such as autonomous vehicles, with 4G LTE Advanced Pro delivering speeds in excess of 3Gbps and less than 2 milliseconds of latency.

5G: 5G cellular technology provides significant enhancements compared to 4G/LTE networks and is backed by ultra-low latency, massive connectivity and scalability for IoT devices, more efficient use of the licensed spectrum, and network slicing for application traffic prioritization.

QUESTION 13

Why is it important to protect East-West traffic within a private cloud?

- A. All traffic contains threats, so enterprises must protect against threats across the entire network
- B. East-West traffic contains more session-oriented traffic than other traffic
- C. East-West traffic contains more threats than other traffic
- D. East-West traffic uses IPv6 which is less secure than IPv4

Correct Answer: A

QUESTION 14

From which resource does Palo Alto Networks AutoFocus correlate and gain URL filtering intelligence?

- A. Unit 52



- B. PAN-DB
- C. BrightCloud
- D. MineMeld

Correct Answer: B

When you enable URL Filtering, all web traffic is compared against the URL Filtering database, PAN-DB, which contains millions of URLs that have been grouped into about 65 categories.

QUESTION 15

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

Correct Answer: C

[PCCET VCE Dumps](#)

[PCCET Practice Test](#)

[PCCET Exam Questions](#)