

# FC0-U51<sup>Q&As</sup>

CompTIA IT Fundamentals+ Certification Exam

## Pass CompTIA FC0-U51 Exam with 100% Guarantee

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

<https://www.pass2lead.com/fc0-u51.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA  
Official Exam Center

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



### QUESTION 1

Which of the following technologies is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet?

- A. Demilitarized zone (DMZ)
- B. Firewall
- C. Intrusion detection system (IDS)
- D. Packet filtering

Correct Answer: C

An Intrusion detection system (IDS) is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet. It can detect several types of attacks and malicious behaviors that can compromise the security of a network and computers. This includes network attacks against vulnerable services, unauthorized logins and access to sensitive data, and malware (e.g. viruses, worms, etc.). An IDS also detects attacks that originate from within a system. In most cases, an IDS has three main components: Sensors, Console, and Engine. Sensors generate security events. A console is used to alert and control sensors and to monitor events. An engine is used to record events and to generate security alerts based on received security events. In many IDS implementations, these three components are combined into a single device. Basically, following two types of IDS are used : Network-based IDS Host-based IDS Answer option D is incorrect. Packet filtering is a method that allows or restricts the flow of specific types of packets to provide security. It analyzes the incoming and outgoing packets and lets them pass or stops them at a network interface based on the source and destination addresses, ports, or protocols. Packet filtering provides a way to define precisely which type of IP traffic is allowed to cross the firewall of an intranet. IP packet filtering is important when users from private intranets connect to public networks, such as the Internet. Answer option B is incorrect. A firewall is a tool to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Answer option A is incorrect. Demilitarized zone (DMZ) or perimeter network is a small network that lies in between the Internet and a private network. It is the boundary between the Internet and an internal network, usually a combination of firewalls and bastion hosts that are gateways between inside networks and outside networks. DMZ provides a large enterprise network or corporate network the ability to use the Internet while still maintaining its security. Reference: "[http://en.wikipedia.org/wiki/Intrusion-detection\\_system](http://en.wikipedia.org/wiki/Intrusion-detection_system)"

---

### QUESTION 2

An employee's new computer came with a free 30-day trial version of antivirus software. The employee's company provides enterprise antivirus software from a different vendor. Which of the following should the employee do in order to use a full version of antivirus software?

- A. Enter the company product key for the antivirus software, enabling the full version.
- B. Uninstall the current version antivirus software and install the company version.
- C. Verify Internet connectivity and run online virus scanning software.
- D. Update the trial antivirus software to the latest version.

Correct Answer: B

### QUESTION 3

A user installed a new scanner on a desktop personal computer without any documentation. The scanner powers on, the lamp turns on, and then the unit stops with a failure light lit.

Which of the following should the user do FIRST?

- A. Go to the scanner manufacturer's website and download the current installation information.
- B. Check the personal computer manufacturer's support website for information about scanner installation.
- C. Find a scanner user group website and ask for help.
- D. Update the scanner firmware and drivers, then reinstall the scanner.

Correct Answer: A

---

### QUESTION 4

After installing the OS on a workstation, a technician notices that everything is displayed in large windows and the viewing area is limited.

Which of the following will the technician need to adjust to resolve this issue?

- A. Color depth
- B. Orientation
- C. DPI settings
- D. Resolution

Correct Answer: D

---

### QUESTION 5

A technician is configuring a wireless router for a small office and the business owner would like the wireless network to be secured using the strongest encryption possible.

Which of the following should the technician choose?

- A. WPA2
- B. WAP

C. WPA

D. WEP

Correct Answer: A

[FC0-U51 PDF Dumps](#)

[FC0-U51 Study Guide](#)

[FC0-U51 Braindumps](#)