

| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

Multiple Choice Questions on Antivirus and Firewall:

1. What is the primary function of antivirus software?

- A. Create malware
- B. Detect and remove malware
- C. Slow down the system
- D. Develop software applications

Answer: B. Detect and remove malware

Explanation: Antivirus software is designed to detect, prevent, and eliminate various types of malicious software from a computer system.

2. Which of the following is NOT considered malware?

- A. Trojan
- B. Worm
- C. Spyware
- D. Compiler

Answer: D. Compiler

Explanation: A compiler is a software development tool, not malware. The rest (Trojan, Worm, Spyware) are types of malware.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

3. What is a common method used by antivirus programs to detect malware?

- A. Data compression
- B. Signature-based scanning
- C. Graphic rendering
- D. Firewall redirection

Answer: B. Signature-based scanning

Explanation: Antivirus programs often use known malware "signatures" to identify threats.

4. Which of the following best describes malware?

- A. Software that boosts system performance
- B. Any software that harms or exploits a system
- C. A type of antivirus
- D. A programming language

Answer: B. Any software that harms or exploits a system

Explanation: Malware refers to malicious software intended to damage or gain unauthorized access to systems.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

5. Why is regular updating of antivirus software important?

- A. To make it use less RAM
- B. To keep user interface modern
- C. To detect the latest security threats
- D. To improve printing capabilities

Answer: C. To detect the latest security threats

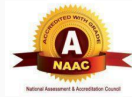
Explanation: New malware is developed frequently; updates help antivirus software recognize and combat the latest threats.

6. What is a false positive in antivirus detection?

- A. Failure to detect malware
- B. Correctly identifying a virus
- C. Legitimate file flagged as malware
- D. Malware that hides itself

Answer: C. Legitimate file flagged as malware

Explanation: A false positive occurs when antivirus software wrongly identifies a harmless file as malicious.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

7. Which one of the following is a preventive feature of antivirus software?

- A. Restoring deleted files
- B. Blocking suspicious websites
- C. Installing operating systems
- D. Encrypting personal files

Answer: B. Blocking suspicious websites

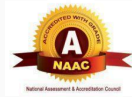
Explanation: Antivirus programs often include web protection features to prevent users from visiting potentially harmful sites.

8. What does antivirus software primarily scan to detect threats?

- A. Only games
- B. Just the internet connection
- C. Files, programs, and system
- D. Social media accounts

Answer: C. Files, programs, and system

Explanation: Antivirus software scans various components of your computer, including files and programs, to find malware.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

9. How does antivirus detect known malware?

- A. By rewriting files
- B. By using malware signatures
- C. Through file compression
- D. By disabling programs

Answer: B. By using malware signatures

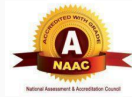
Explanation: It compares data against a database of known malware "signatures" to identify threats.

10. What does antivirus software do when it finds something harmful?

- A. Ignores it
- B. Turns off your computer
- C. Quarantines or deletes it
- D. Shares it online

Answer: C. Quarantines or deletes it

Explanation: Antivirus can isolate (quarantine) the threat or remove (delete) it entirely from the system.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

11. What happens if your system doesn't have antivirus protection?

- A. Your system becomes faster
- B. You can install more apps
- C. Malware can infect your system easily
- D. It increases internet speed

Answer: C. Malware can infect your system easily

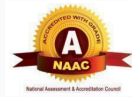
Explanation: Without antivirus protection, there's no active defense to stop malicious software from entering your system.

12. What is the role of antivirus software in cybersecurity?

- A. It encrypts all your files
- B. It creates firewalls
- C. It acts as the first line of defense
- D. It manages user passwords

Answer: C. It acts as the first line of defense

Explanation: Antivirus software is the initial protection layer against malware threats.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

13. What does suspicious behavior detection involve?

- A. Guessing passwords
- B. Watching videos
- C. Monitoring unusual system activity
- D. Installing updates automatically

Answer: C. Monitoring unusual system activity

Explanation: Antivirus software detects unfamiliar or suspicious actions that might indicate a new or unknown threat.

14. What is "quarantining" in antivirus terms?

- A. Locking the whole computer
- B. Moving a suspected file to a safe, isolated area
- C. Deleting all files from the system
- D. Sending files to the cloud

Answer: B. Moving a suspected file to a safe, isolated area

Explanation: Quarantine prevents the suspicious file from harming the system while keeping it separate for further analysis.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

15. What kind of threats does antivirus software protect against?

- A. Hardware malfunctions
- B. Natural disasters
- C. Malware like viruses, worms, and trojans
- D. Internet speed throttling

Answer: C. Malware like viruses, worms, and trojans

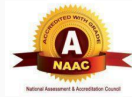
Explanation: Antivirus software targets malicious software designed to harm or exploit systems.

16. How often should antivirus software be updated?

- A. Once a year
- B. Only after malware is found
- C. Regularly, to recognize new threats
- D. Never, it updates automatically

Answer: C. Regularly, to recognize new threats

Explanation: Frequent updates ensure that the antivirus can detect the latest malware strains and variants.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

17. What does signature-based detection use to identify malware?

- A. File size
- B. Internet speed
- C. Known code patterns
- D. User passwords

Answer: C. Known code patterns

Explanation: Signature-based detection compares files to a database of unique code patterns that match known malware.

18. What is a major advantage of signature-based detection?

- A. It works offline
- B. It identifies hardware problems
- C. It is fast and accurate for known threats
- D. It prevents unauthorized user logins

Answer: C. It is fast and accurate for known threats

Explanation: Since it uses pre-identified signatures, it can quickly and accurately detect malware it already knows.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

19. What does the term "malware signature" refer to?

- A. The malware's author
- B. A file's expiration date
- C. A unique pattern of code in the malware
- D. The malware's sound pattern

Answer: C. A unique pattern of code in the malware

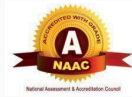
Explanation: A malware signature is a specific set of instructions or code that identifies a particular malware strain.

20. Why might signature-based antivirus miss zero-day malware?

- A. It doesn't scan files
- B. It doesn't recognize new, unseen code
- C. Zero-day malware doesn't use code
- D. Antivirus isn't allowed to update

Answer: B. It doesn't recognize new, unseen code

Explanation: Zero-day malware uses unknown code or modified versions that aren't yet in the signature database.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

21. What is a "sandbox" in cybersecurity?

- A. A gaming feature
- B. A type of firewall
- C. An isolated environment to test files
- D. A cloud storage platform

Answer: C. An isolated environment to test files

Explanation: A sandbox is a secure, virtual space where suspicious files can be executed and observed without risking the actual system.

22. What is the main purpose of sandboxing in malware detection?

- A. To compress files
- B. To observe file behavior safely
- C. To delete system logs
- D. To improve graphics performance

Answer: B. To observe file behavior safely

Explanation: Sandboxing allows security tools to run and study potentially dangerous files without harming the main system.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

23. Which type of malware is best detected using sandboxing?

- A. Basic viruses
- B. Malicious browser extensions
- C. Complex or hidden threats
- D. Outdated programs

Answer: C. Complex or hidden threats

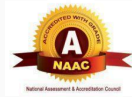
Explanation: Sandboxing is effective for detecting sophisticated malware that hides its true behavior until executed.

24. What is a disadvantage of sandbox-based detection?

- A. It only works on Linux
- B. It doesn't detect any threats
- C. It is resource-heavy and time-consuming
- D. It disables antivirus software

Answer: C. It is resource-heavy and time-consuming

Explanation: Because it actually runs files in a virtual environment, sandboxing requires significant time and system resources.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

25. How does sandboxing help prevent infection?

- A. By hiding malware from the user
- B. By delaying file access
- C. By isolating and testing files before they reach the system
- D. By locking down all ports

Answer: C. By isolating and testing files before they reach the system

Explanation: Suspicious files are executed in a sandbox first, preventing potential threats from affecting the real system.

26. What is the primary role of data mining in malware detection?

- A. Compressing files
- B. Installing software updates
- C. Finding unusual patterns in large data sets
- D. Formatting hard drives

Answer: C. Finding unusual patterns in large data sets

Explanation: Data mining involves analyzing massive data to detect patterns that might indicate malware behavior.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

27. What is one major advantage of using data mining techniques in malware detection?

- A. It detects only known malware
- B. It reduces system performance
- C. It can identify new, unknown threats
- D. It disables outdated programs

Answer: C. It can identify new, unknown threats

Explanation: Data mining helps uncover patterns that may not match any known malware signature.

28. What type of malware detection can find hidden patterns that other methods might miss?

- A. Signature-based
- B. Data mining-based
- C. Sandbox-based
- D. Manual scanning

Answer: B. Data mining-based

Explanation: Data mining excels at identifying subtle and hidden malicious patterns within large datasets.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

29. Why does data mining require large amounts of data?

- A. To increase battery life
- B. To reduce file size
- C. To find reliable and accurate behavioral patterns
- D. To boost download speed

Answer: C. To find reliable and accurate behavioral patterns

Explanation: More data improves the accuracy of pattern recognition and reduces the chance of errors.

30. What can false positives in malware detection lead to?

- A. Better performance
- B. Safe files being wrongly flagged as threats
- C. Decreased antivirus updates
- D. More secure file deletion

Answer: B. Safe files being wrongly flagged as threats

Explanation: False positives are instances where clean files are mistakenly identified as malware.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

31. Which of the following technologies supports data mining in malware detection?

- A. Blockchain
- B. Artificial Intelligence / Machine Learning
- C. Disk Defragmentation
- D. Virtual Private Networks (VPNs)

Answer: B. Artificial Intelligence / Machine Learning

Explanation: AI and ML are key to enabling data mining techniques to analyze behaviors and detect threats intelligently.

32. What is the primary goal of heuristic-based malware detection?

- A. To compare files to known signatures
- B. To remove duplicate files
- C. To analyze code and behavior for suspicious patterns
- D. To clean temporary files

Answer: C. To analyze code and behavior for suspicious patterns

Explanation: Heuristics focuses on detecting potential threats by examining how programs behave or how their code is structured.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

33. What is one key advantage of heuristic detection?

- A. It only works offline
- B. It guarantees no false alarms
- C. It can detect unknown or modified malware
- D. It doesn't need a processor

Answer: C. It can detect unknown or modified malware

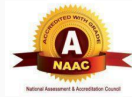
Explanation: Because it doesn't rely solely on known signatures, heuristic analysis can identify new, altered, or emerging threats.

34. What is a common drawback of heuristic-based detection?

- A. Requires no system memory
- B. Produces false positives
- C. Only scans images
- D. Ignores suspicious behavior

Answer: B. Produces false positives

Explanation: Heuristics may mistakenly classify harmless files as malicious based on behavior or code similarity.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

35. What does "false positive" mean in the context of heuristic detection?

- A. A malicious file is ignored
- B. A safe file is wrongly flagged as malware
- C. The malware disables the scanner
- D. A file is removed from quarantine

Answer: B. A safe file is wrongly flagged as malware

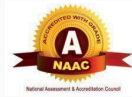
Explanation: Heuristic analysis may sometimes wrongly interpret harmless code as suspicious.

36. What kind of malware can heuristic detection help catch that signature-based cannot?

- A. Known worms
- B. Standard adware
- C. Zero-day or modified malware
- D. Outdated antivirus definitions

Answer: C. Zero-day or modified malware

Explanation: Heuristics are valuable for catching new threats that don't yet have known patterns.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

37. What does real-time protection do?

- A. Deletes files every hour
- B. Monitors system activity continuously
- C. Backs up all photos
- D. Closes background apps

Answer: B. Monitors system activity continuously

Explanation: Real-time protection keeps an eye on system activity to detect threats as they happen.

38. When does real-time malware protection take action?

- A. Once a week
- B. During software updates
- C. As soon as a threat is detected
- D. Only when the system restarts

Answer: C. As soon as a threat is detected

Explanation: Real-time protection reacts immediately when a suspicious activity or file is found.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

39. What is the main benefit of real-time protection?

- A. Speeds up system performance
- B. Removes old drivers
- C. Immediate defense against threats
- D. Encrypts passwords

Answer: C. Immediate defense against threats

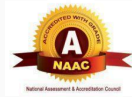
Explanation: It can stop malware before it causes damage by acting instantly.

40. What is one downside of real-time protection?

- A. Deletes harmless files
- B. Requires no internet
- C. May slow down system performance
- D. Can't detect viruses

Answer: C. May slow down system performance

Explanation: Constant monitoring can use system resources, sometimes reducing speed.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

41. What does real-time protection require to stay effective?

- A. Cloud storage
- B. Constant updates
- C. Printer connection
- D. Video card drivers

Answer: B. Constant updates

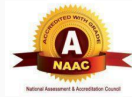
Explanation: It needs up-to-date threat definitions to detect and block the latest malware

42. Which tool uses real-time protection?

- A. Paint
- B. Calculator
- C. Antivirus software
- D. Media player

Answer: C. Antivirus software

Explanation: Antivirus software often includes real-time monitoring features.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

43. What can improve real-time protection's accuracy?

- A. Using headphones
- B. Removing desktop icons
- C. Keeping antivirus updated
- D. Turning off Wi-Fi

Answer: C. Keeping antivirus updated

Explanation: Updated definitions allow real-time protection to detect new and emerging threats.

44. What is a firewall used for?

- A. Playing video games
- B. Controlling internet speed
- C. Blocking harmful data and allowing safe data
- D. Editing documents

Answer: C. Blocking harmful data and allowing safe data

Explanation: A firewall protects systems by filtering incoming and outgoing network traffic.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

45. A firewall acts like a_____.

- A. Music player
- B. Web browser
- C. Gatekeeper for data
- D. Virus scanner

Answer: C. Gatekeeper for data

Explanation: A firewall checks data that tries to enter or leave a network, blocking unsafe content.

46. What type of threats can a firewall help block?

- A. Text formatting issues
- B. Hackers and viruses
- C. Slow internet
- D. File compression

Answer: B. Hackers and viruses

Explanation: Firewalls prevent unauthorized access from attackers and block suspicious data.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

47. What do firewalls primarily control?

- A. Keyboard layout
- B. Incoming and outgoing network traffic
- C. Screen brightness
- D. Battery life

Answer: B. Incoming and outgoing network traffic

Explanation: Firewalls monitor both inbound and outbound data to protect the system.

48. Which of the following can a firewall allow?

- A. All files from unknown sources
- B. Unsafe software
- C. Authorized or safe data
- D. Viruses from websites

Answer: C. Authorized or safe data

Explanation: Firewalls are designed to let only trusted data pass through.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

49. What could happen without a firewall?

- A. Your PC becomes waterproof
- B. Your battery lasts longer
- C. Hackers may gain access to your system
- D. You lose your keyboard

Answer: C. Hackers may gain access to your system

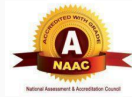
Explanation: Without a firewall, there's no filter to block unauthorized or harmful access.

50. Firewalls are important for_____.

- A. Increasing storage
- B. Making backups
- C. Network security
- D. Improving screen resolution

Answer: C. Network security

Explanation: Firewalls are key components of protecting networks and systems from external threats.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

51. What is a software firewall?

- A. A physical wall in your house
- B. A program that controls internet traffic on a device
- C. A type of computer virus
- D. A printer driver

Answer: B. A program that controls internet traffic on a device

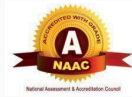
Explanation: Software firewalls monitor and control data coming into and going out of a single device.

52. Where is a software firewall installed?

- A. On a network router
- B. On a computer or device
- C. In the cloud
- D. On a printer

Answer: B. On a computer or device

Explanation: Software firewalls run directly on the device they protect.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

53. Which of the following is an example of a software firewall?

- A. Windows Defender Firewall
- B. Ethernet cable
- C. USB flash drive
- D. External hard drive

Answer: A. Windows Defender Firewall

Explanation: Windows Defender Firewall is a common built-in software firewall on Windows computers.

54. Software firewalls are generally easier to install and manage for_____.

- A. Large corporations only
- B. Individual users and small businesses
- C. Internet providers
- D. Hardware manufacturers

Answer: B. Individual users and small businesses

Explanation: They are designed for easy setup on personal computers or small office networks.



| | | | |
|---------------------------|------------------------|------------------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

55. What is a hardware firewall?

- A. A software program on your computer
- B. A physical device that filters network traffic
- C. A type of antivirus
- D. A cloud service

Answer: B. A physical device that filters network traffic

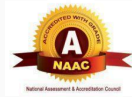
Explanation: Hardware firewalls are physical devices placed between your network and the internet.

56. Where is a hardware firewall usually located?

- A. Inside your computer's hard drive
- B. Between your local network and the internet
- C. Inside a USB flash drive
- D. On a website

Answer: B. Between your local network and the internet

Explanation: It acts as a barrier controlling traffic coming in and out of your network.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

57. Which of the following is an example of a hardware firewall?

- A. Windows Defender
- B. Cisco ASA
- C. Google Chrome
- D. Microsoft Word

Answer: B. Cisco ASA

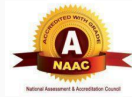
Explanation: Cisco ASA is a popular hardware firewall device used by businesses.

58. Hardware firewalls are often used in ____.

- A. Small personal laptops only
- B. Offices and large networks
- C. Single smartphones
- D. Video games

Answer: B. Offices and large networks

Explanation: They are designed to protect large networks with many devices.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

59. What does a hardware firewall primarily do?

- A. Plays music
- B. Filters and controls network traffic
- C. Updates software automatically
- D. Increases computer memory

Answer: B. Filters and controls network traffic

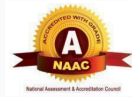
Explanation: It monitors and blocks unauthorized or harmful network connections.

60. Which network component often includes a hardware firewall?

- A. Router
- B. Keyboard
- C. Monitor
- D. Printer

Answer: A. Router

Explanation: Many routers have built-in hardware firewall features.



| | | | |
|--------------------|------------------------|-----------------|-------------------|
| Name of the Bundle | Proficient Bundle V1 | Subject | Networking V1 |
| Topic | Antivirus and Firewall | Last updated on | 11 September 2025 |

61. The Cisco ASA is an example of ____.

- A. Hardware firewall
- B. Antivirus software
- C. Web browser
- D. Operating system

Answer: A. Hardware firewall

Explanation: Cisco ASA is a widely used hardware firewall appliance.

62. A hardware firewall helps prevent ____.

- A. Unauthorized access to the network
- B. Running out of disk space
- C. Computer overheating
- D. Slow screen refresh rate

Answer: A. Unauthorized access to the network

Explanation: It blocks hackers and unwanted traffic from entering your network.