Difference between Antivirus and Firewall

The key difference between Antivirus and Firewall is that an antivirus is not capable of engaging in counter-attacks, whereas a firewall can be engaged in counter-attacks. These comparisons are important for the GATE CSE exam. Check the table below for a detailed comparison of the two defense techniques against malicious software.

Antivirus vs Firewall

Antivirus and Firewall

Antivirus	Firewall
Antivirus protects the system from internal attacks like spyware, virus, trojan horses, etc.	A Firewall is a security wall that protects the systems from harmful invasions.
Regularly scans the system to make necessary adjustments to improve the system's defense mechanism.	It is also known as a 'packet filter' as it regularly filters the potentially harmful incoming data.
Antivirus cannot verify read-only files.	A firewall cannot perform the duty of an Antivirus, i.e., it cannot prevent internal attacks.
Antivirus is only available in the form of software.	It can be in the form of hardware, software, or both.
Antivirus cannot engage in counter-attacks.	As a form of counter-attack, it can engage in IP spoofing and routing attacks.
Antivirus programming is simpler as compared to the Firewall.	A Firewall's programming is very complex.

Antivirus and Firewall Protection

Many efficient antiviruses are available in the marketplace, like McAfee Antivirus Plan, Webroot Secure Anywhere, Norton 360, Avast Free Antivirus, Trend Micro Antivirus security, etc. A firewall is also known as a 'packet filter'. If a threat is found, Antivirus employs security measures like fixing or deleting the virus.

What is Antivirus?

A cybersecurity mechanism that identifies and removes internal threats in a computer or internet system. Antivirus deals with threats like worms, viruses, trojans, spyware, malware, etc. It regularly scans programs and files that can carry potential threats in the form of viruses.

Generations of Antivirus

- The 1st generation was specific to detecting the signature-specific virus.
- The 2nd generation improved quickly and moved ahead from identifying the signature-specific virus. It used a more heuristic approach to identify viruses.
- The 3rd generation started using memory-resident antivirus software programs.
- The 4th generation uses multiple ways to detect viruses like scanning, monitoring, deleting, etc.

What is Firewall?

A firewall protects the system from incoming traffic that can harm the network. With the internet connecting millions of networks globally, Firewall protection is becoming increasingly important. A firewall uses pre-determined rules and regulations to analyze and filter all incoming data.

Types of Firewalls

Packet Filters

- Screens and filters all the incoming data.
- Also engages in counter-attacks like IP spoofing, source routing attacks, etc.
- Packet filters are divided into dynamic packet filters and stateful packet filters.

Application Gateway

- They are also known as proxy servers, as they control the flow of incoming traffic and communication.
- They also conceal the originating IP address for outside and public networks.

Circuit Gateway

It is almost similar to an application gateway; however, they can convert the origination IP address into small packets to conceal it efficiently.