Some of the limitations of a firewall are as follows:

* **Exploitable programming bugs:** Whether a firewall is a software- or hardware-based, a firewall is run by software written by people, so there are chances of code errors being introduced.
* **Buffer overflow:** A buffer overflow occurs when a program tries to store too much data in a buffer, exceeding the buffer’s capacity. The overflow is usually the result of poor programming and can result in memory-based and code injection attacks and, consequently, system crashes.
* **Fragmentation:** Most packets or datagrams are broken into smaller packets before being transferred over a network. Fragmentation occurs when packets are improperly reassembled at the destination. Attackers can infiltrate the reassembly process, resulting in overlapping packets and overrun packets, both of which can be used in attacks.
* **Firewalking:** It is a technique used by an external attacker to learn about a firewall’s configuration. Then, the attacker can find ways to bypass the firewall to reach the internal network.
* **Internal code planting:** Attackers place malicious code on an internal system or trick an internal user into opening a malicious program or clicking a malicious link. The results in an internally initiated connection to a malicious Internet site, which can infect the internal system or network.
* **Denial of service (DoS):** It is an attack that floods a firewall and network with requests, overwhelming it and resulting in system shutdown.