Hi All, Thanks for participating in this discussion. I have to agree that the Firewall should be considered as a first layer of defence. Demian makes an interesting point regarding Pi-Hole software. I have never heard of this software, so thank you for sharing.

I am familiar with Iptables on the Linux platform which compares the network traffic against a set of rules, such as an address or port. These rules determine an action called a target and can either drop or accept the data packet. However, as the Internet Protocol (IP) version 4 has a limited number of addresses available, each device has to have its own IP in order for network communication to work. IP version 6 was therefore introduced to overcome this problem. This also introduced a new version of ip6tables then nftables within the Linux Operating System environment and the underlying processing of all of these is done by the kernel via netfilter. Unfortunately, even with all of these software upgrades, Nick Gergory found and reported a bug CVE-2022025636 "The bug is exploitable to achieve kernel code execution (via ROP), giving full local privilege escalation, container escape, whatever you want." [https://nickgregory.me/, 2022].

It is not only software that is at risk. Cisco hardware has also been identified as having multiple risks which can cause denial of service.

"Positive Technologies has previously discovered vulnerabilities in Cisco Firepower Device Manager (FDM) On-Box and critical flaws in Cisco ASA, such asCVE-2020-3187, CVE-2020-3259, and CVE-2020-3452" [Williams,S 2021].

As I have previously stated, I agree that Firewalls should be considered as the first layer of defence, however; there should be a dedicated team in place to ensure that this first layer is bug free and maintained regularly.

Gregory, N (12 March 2022)The Discovery and Exploitation of CVE-2022-25636. Available from : https://nickgregory.me/linux/security/2022/03/12/cve-2022-25636/ [Accessed 15 April 2022]

Williams,S (24 November 2021) Vulnerability in Cisco security devices could cause firewalls to fail. Available from : https://securitybrief.com.au/story/vulnerability-in-cisco-security-devices-could-cause-firewalls-to-fail [Accessed 15 April 2022]