Abstract—In Today’s Digital World, the continuous interruption of users has affected Web Servers (WSVRs), through Distributed Denial-of-Service (DDoS) attacks. These attacks always remain a massive warning to the World Wide Web (WWW). These warnings can interrupt the accessibility of WSVRs, completely by disturbing each data processing before intercommunication properties over pure dimensions of DataDriven Networks (DDN), management and cooperative communities on the Internet technology. The purpose of this research is to find, describe and test existing tools and features available in Linux-based solution lab design Availability Protection System (Linux-APS), for filtering malicious traffic flow of DDoS attacks. As source of malicious traffic flow takes most widely used DDoS attacks, targeting WSVRs. Synchronize ( SYN), User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) Flooding attacks are described and different variants of the mitigation techniques are explained. Available cooperative tools for manipulating with network traffic, like; Ebtables and Iptables tools are compared, based on each type of attacks. Specially created experimental network was used for testing purposes, configured filters servers and bridge. Inspected packets flow through Linux-kernel network stack along with tuning options serving for increasing filter server traffic throughput. In the part of contribution as an outcomes, Ebtables tool appears to be most productive, due to less resources it needed to process each packet (frame). It is pointed out that separate detecting system is needed for this tool, in order to provide further filtering methods with data. As main conclusion, Linux-APS, solutions provide full functionality for filtering malicious traffic flow of DDoS attacks either in standalone state or combined with detecting systems. Keywords—DDoS attacks; floods detection; Linux-APS architecture; mitigation techniques; network traffic; Netfilter;