

FFPF: Fairly Fast Packet Filters

Willem de Bruijn[†]

[†]Vrije Universiteit Amsterdam, The Netherlands
{wdb}@few.vu.nl

Abstract

FFPF is a network monitoring framework designed for three things: speed (handling high link rates), scalability (ability to handle multiple applications) and flexibility. Multiple applications that need to access overlapping sets of packets may share their packet buffers, thus avoiding a packet copy to each individual application that needs it. In addition, context switching and copies across the kernel boundary are minimised by handling most processing in the kernel or on the network card and by memory mapping all buffers to userspace, respectively. For these reasons, FFPF has superior performance compared to existing approaches such as BSD packet filters, and especially shines when multiple monitoring applications execute simultaneously. Flexibility is achieved by allowing expressions written in different languages to be connected to form complex processing graphs (not unlike UNIX processes can be connected to create complex behaviour using pipes). Moreover, FFPF explicitly supports extensibility by allowing new functionality to be loaded at runtime. By also implementing the popular pcap packet capture library on FFPF, we have ensured backward compatibility with many existing tools, while at the same time giving the applications a significant performance boost.