

# Performance Improvement over Linux Layer-7 Content Filtering

彭炳衡, 劉懷仁, 魏煥雲

Computer Science & Information Engineering

Computer Science and Informatics

hjliu@chu.edu.tw

## Abstract

Due to security reasons, many companies need firewalls to filter some mistrusted applications, like FTP or P2P software. However, some applications may hide themselves with some well-known application ports like HTTP port 80 such that some firewalls cannot distinguish mistrusted applications from well-known applications. As a result, firewalls require high performance classification engines that can efficiently inspect layer-7 contents to recognize mistrusted applications. This paper analyzes the layer-7 classification module in Linux Netfilter, the L7filter package, and proposes an alternative implementation to improve the performance of L7filter. The throughput of the proposed method can remain high even in heavily-loaded network environments. The performance of the proposed method is justified by the Spirent SmartBits 6000 testing equipment whose traffic generation speed can achieve gigabit wire-speed.

Keyword : Firewall, Packet Classification, Content Filter