

Holistic Optimisation of Access Control Lists

John McGinn and Vic Grout

The efficient implementation and optimization of *individual* Internet Access Control Lists (ACLs) has been widely discussed. Less attention has been paid, to date, to the question of how these packet filters *interact* throughout a domain. A rule in a given ACL may be effectively redundant, not merely as a result of its position in the list, but through its placement in the domain. As a simple example, if a rule filtering traffic from a source network is found on two successive interfaces, and the only route to the second interface is from the first, then the second rule is redundant and can be removed, making the processing of the ACL more efficient. Further improvements may be achieved through moving rules among lists through similar arguments.

This paper discusses various manifestations of rule redundancy and opportunities for mobility in a distributed environment, formulates the optimisation problem associated with reducing overall ACL processing, considers its complexity and offers a number of simple heuristics, with experimental results, for its solution.

- [1] Varghese, G., *Network Algorithmics*, Elsevier/Morgan Kaufmann, 2005.
- [2] Grout, V., Davies, J. & McGinn, J., "An Argument for Simple Embedded ACL Optimisation", *Computer Communications*, Vol. 30, No. 2, January 2007, pp280-287.
- [3] Grout, V., McGinn, J. & Davies, J., "Real-time Optimisation of Access Control Lists for Efficient Internet Packet Filtering", *Journal of Heuristics*, Vol. 13, No. 5, October 2007, pp435-454.