

# Firewalls in a P2P World

Germano Caronni  
*Sun Microsystems*  
[caronn@ibatfax.olymp.org](mailto:caronn@ibatfax.olymp.org)

## Abstract

The past decade has seen a strong opening of company networks towards the Internet. Nearly every organization has some web presence, does some business by email (internally and externally) and many allow their employees access to the Internet from the office.

Firewalls (acting as filter and proxy for network traffic) were supposed to be the magic all-encompassing solution to regulate this opening, and not expose the internal infrastructure to the public. But there are problems. The request for transparency and higher accessibility has been getting stronger. Firewalls process more and more traffic, and have to enforce more complex (and harder to formulate) restrictions. They are supposed to offer more and more functionality, and they get harder to use all the time. This way, firewalls are becoming a source of faults themselves, and a security risk.

P2P Environments reinforce the issues, by potentially opening up many portals between different types of networks. Drive-by hacking in the wireless ethernet world is just one example of this. How do you decide who is going to be a member of your little ad hoc network, and whether users can employ any of the devices participating to hop on (or get routed to) a network they are not supposed to get to? Are there alternatives for classic firewalls? Do they apply to the P2P world? Do they fit the current scenario of ever-increasing mobility and ad hoc intermeshing of our computing environment?

The talk explores the rise of firewalls, their evolution and tendencies in this area, and has a look at their strengths and weaknesses. Some alternative solutions are examined, and a vision of a potential future solution is presented.