**Managing ACLs of servers and network devices using shared XML-based ruleset**

As networks get more and more complex, the need of uniformly handling different kinds of Access Control Lists arises. (It is not always easy to answer questions like 'Why is this particular service/port unavailable?' or even 'Why is it unprotected?').
Network-level filtering is usually implemented in two places: on the server (workstation) itself, or on the network device just before (the `last hop': usually a switch or router). The concept gives a solution for handling these two layers uniformly, using an XML structure stored in a common LDAP directory. Thus it is possible to manage ACLs – which used to be the privilege of 'gurus' – by a (security-)administrator, without the detailed knowledge of the applied device.
Basics of the ACL system are implementation- and platform-independent. Context-dependent tasks (such as defining a specific rule) are performed by implementation-specific agents.