Defeasible Logic Programming for Firewall Verification and Reconfiguration

Pritom Rajkhowa[1], Guillermo R. Simari[2] and Shyamanta M. Hazarika[1]

[1] Computer Science & Engineering
Tezpur University, Tezpur 784028, India.
{pritomr,smh}@tezu.ernet.in
[2] Computer Science & Engineering
Universidad Nacional del Sur, Bahia Blanca, Argentina.
grs@cd.uns.edu.ar

Abstract. Firewalls are frontier defense in network security providing a set of rules that identify how to handle individual data packets arriving at the firewall. Placed betweeen a private network and the public network, it inspects all incoming and outgoing traffic; blocking or allowing packets based on the security requirements of the private network. The large number of rules and their inevitable interdependencies; as also ever changing network environments and the resulting security requirements make firewall configuration and management increasingly difficult. Filter properties called *anomalies* hint at possible conflicts between rules. An argumentation framework could provide ways of handling such conflicts. Verification of a firewall involves finding out whether anomalies exist or not. Reconfiguration involves removing critical anomalies discovered in the verification phase. In this paper, we show how a Defeasible Logic Programming approach with an underlying argumentation based semantics could be applied for verification and reconfiguration of a firewall.