

## **VPN BASED APPROACH TO CENTRALIZED MANAGEMENT OF NOTEBOOK ACCESS TO MASARYK UNIVERSITY NETWORK**

Michal Heppler, Lukáš Rychnovský and Jaroslav Šeděnka

Ústav výpočetní techniky Masarykovy univerzity, Botanická 68a, 602 00 Brno, Česká republika

mhepp@ics.muni.cz

rychnovsky@ics.muni.cz

jarek@ics.muni.cz

Achieving centralized, reliable and easy-to-set-up control of notebooks' access to university network is a challenging task. In every modern organization flexible and efficient user support is necessary. In this case only distributed support is suitable as some issues can only be solved directly on users' notebooks. Per-user firewall configuration, accountability, communication encryption and P2P handling are some of the problems solved by our virtual private network.

We chose Linux and open source (OpenLDAP, Radius, Poptop, MySQL) as the underlying technology, and developed the missing parts on our own. The in-house developed pieces are integration with university user database, web-based management interface, log parser (periodically run script that converts all text logs to database) and integration with intrusion detection system. Our VPN allows utilizing existing or low-cost network hardware (mainly access points and switches) and easy deployment – Windows 2000/XP clients can be configured by downloading and executing a single dial-up configuration file. Information about infected IP addresses is received in emails from an intrusion detection system (the IDS itself will not be covered in this paper), corresponding users are found out from logs, and are notified. Firewall rules are adjusted accordingly without need for manual intervention.

In the article, we present the core parts of our VPN infrastructure, its administration interface and design changes that were necessary to withstand the growing usage of the VPN service. The most important changes were disabling all P2P networks because of the performance issues and dedicating one server only to tunnel the traffic from clients. The VPN has been used for more than four years, has more than 4.000 active accounts, peaks to almost 400 concurrent connections and handles more than 60.000 connections per month.